The United States Responds to Spam

Janice C. Sipior, Ph.D.
Villanova University
janice.sipior@villanova.edu

Burke T. Ward, J.D., LL.M.
Villanova University
burke.ward@villanova.edu

P. Gregory Bonner, Ph.D.
Villanova University
gbonner@email.vill.edu

***Abstract*-In the United States, spam, unsolicited bulk or commercial e-mail, is considered to be a significant problem for both consumers and Internet Service Providers. It is currently attracting a patchwork of state level legislative actions as well as proposed federal legislative initiatives. While spam engenders numerous policy concerns, two issues, the jurisdictional domain and the transfer of costs, appear to be unique to spam.**

I. Introduction

For direct marketing, e-mail is a unique medium, offering a low cost means to individually target members of either a small or large market. When used in a mutually agreeable manner, it has the potential to lower overall transaction costs, making the exchange process more efficient for both parties. However, e-mail users have been inundated with spam, also known as "junk e-mail," unsolicited bulk e-mail (UBE), and unsolicited commercial e-mail (UCE). While primarily utilized for commercial purposes, spam may also promote political, malicious, or illegal schemes.

Spam is estimated to account for about 10% of all Internet e-mail [7] and commercial e-mail is expected to reach 250 billion messages by 2002, according to Forrester Research [33]. This growth has been cited as indicative of a change in consumer attitudes toward increasing acceptance. "People are becoming accustomed to e-mail from an e-commerce entity" claims Jim Williams, CEO and president of MarketHome, an "opt-in" e-mail marketing company which collects dedicated e-mail lists for clients such as Coach and Park Seed [1]. An opt-in approach, wherein consumers consent to receive e-mail marketing communications as long as the content is of interest and the volume is acceptable, elicits a more positive response [18]. Unsolicited e-mail, announcing sales, product updates, or desirable information for business or personal use, may be perceived as less offensive if accompanied with the option to "opt-out." This option provides the opportunity to the consumer to request to be removed from the e-mail list. According to H. Robert Wientzen, President and CEO of the Direct Marketing Association (DMA), the largest trade association for businesses in database and interactive marketing, "when (e-mail is) used in a targeted and respectful fashion, it's a powerful marketing tool, especially when the recipient is a customer or someone requesting information" [14].

However, not all e-mail marketers are scrupulous. The unsolicited nature, transfer of costs, content and volume are what make spam offensive, even with the opportunity to opt-out. Direct marketers can engage in unwanted and even annoying e-mail advertising campaigns tailored to the individual, claiming that consumers want to be informed about product and service offerings [15]. More than half of the members of the DMA reportedly utilize the Internet and the Web for advertising and 48% have reported using membership rosters of major computer online services to obtain e-mail addresses [13]. Information collected for one purpose can easily be combined with other information, providing a detailed set of consumer characteristics for identifying and reaching particular market segments [17]. The unacceptability of such marketing activity is revealed by a survey which reported 51% of respondents stated they would be concerned if an interactive service, to which they subscribed, created subscriber profiles by collecting usage and purchasing patterns to advertise to subscribers [27].

This paper discusses the concerns of both consumers and Internet Service Providers (ISP) with spam. Initiatives intended to balance the interests of consumers and ISPs with those of direct marketers are examined. Among these initiatives are several legislative bills proposed at the federal level, indicative of the growing support to restrict spam. Finally, recommendations addressing the differing perspectives are presented.

II. Concerns Associated with Spam

Concerns about spam have been steadily increasing along with its increasing presence [9]. Junk e-mail was identified as a problem as early as 1975 [26]. However, it was not until 1994 that spam began to proliferate, after the law firm of Canter and Siegel spammed more than 6,000 Usenet newsgroups with broadcast e-mail [6]. Spam has since become a recognized controversy due to concerns associated with consumer privacy; spammers' use of false e-mail identities; questionable message content; enticing, deceptive, or fraudulent presentations; and the transfer of costs to both consumers and Internet Service Providers (ISPs).

A. Privacy

One of the most objectionable aspects of unsolicited commercial e-mail to consumers is the violation of their privacy [29]. "Most people see their e-mail box as their personal space" [20]. Without having provided permission to receive promotional e-mail by opting-in, the consumer is likely to see unsolicited commercial e-mail as a violation of privacy [18]. The spammer has the capability to reach a consumer's e-mail box, for which that consumer may be paying a fee, without his consent.

B. Use of False E-mail Identities

The primary motivation for using false e-mail identities is to increase the likelihood that spam received is read. A recognized spam address can be filtered and blocked by an ISP or deleted by the recipient. Some spammers routinely misrepresent return e-mail addresses and headers, which contain the domain names of the message's origin, route traveled, and final destination, to conceal their identity.

C. Questionable Message Content

Although content is not the most objectionable aspect of spam, in that it is present in other media, it is still an important determinant of the acceptability of the message to the recipient. A brief message, comprised of no more than four sentences coupled with a URL link to a website, has been found to be the most effective in achieving a high response rate [37]. The message simply announces the availability of an offer on a website and presents a point and click opportunity as an easy way for the consumer to access additional information. A comparison test of such messages with those containing seven to eight sentences, coupled with a set of bulleted promotional points, revealed a 30% higher response rate [37].

D. Enticement, Deception, or Fraud

Another content issue for spam deals with the consumer's interpretation and response to the e-mail presentation. Spammers often use enticement, deception, or fraud to encourage recipients to, at a minimum, open their messages. An innocuous subject line or the misrepresentation of the return address and header may fool the recipient into opening the message. Incentive systems may encourage recipients to read messages. For example, Experian, a database marketer, entices opt-in registrants to earn points, redeemable for merchandise, in exchange for reading their e-mail [1]. This seemingly acceptable and innocent enticement could potentially be utilized for deceptive or fraudulent purposes. Many of the offers presented in spam are scams according to the United States Federal Trade Commission [16].

E. Costs to Consumers

The subscription cost for an ISP, providing access to the Internet including the World Wide Web and e-mail among other services, may include a fee based on connect time. For example, 15% of the customers of the largest ISP in the United States, AOL, currently pay a fee for connect time [2]. Under such circumstances, the subscriber incurs direct charges from the ISP, for the time spent online accessing, scanning, reading, or discarding spam. It has been estimated to cost $.50 per message to contend with spam [19]. Other costs are also incurred. Valuable time, which could otherwise be devoted to business or leisure activities, is spent on this unwanted activity. The mailbox of the consumer may become so filled with spam that new, and perhaps important, messages arriving cannot be delivered. The consumer is thereby forced to attend to sifting through unsolicited messages in order to free up space before accessing his own correspondence. Consumers choosing to opt-out must still spend time registering for this option. The advertiser may thus be shifting part of the cost of advertising to unwilling recipients.

F. Costs to Internet Service Providers

Several costs to ISPs may be imposed by spam. The increased load on the mail server processor requires the devotion of additional CPU time, an expensive resource. Spam can overload the server and cause it to slow or even crash. For example, AT&T WorldNet's e-mail system was overwhelmed with spam in July 1997, causing delays of several hours in the delivery of legitimate e-mail [31]. Other large ISPs, including Pacific Bell Internet and Ameritech Net, have experienced similar delays [34]. While the delays for large providers span hours, small providers may be unable to recover for days. These occurrences carry the additional cost of personnel for customer complaint resolution and the associated impact on the ISP's reputation. Personnel time must also be devoted to rerouting undeliverable mail, as previously discussed.

The increase in the volume of traffic attributable to spam may necessitate an ISP to invest in additional personnel, faster connections, increased processing power, more storage space, and perhaps e-mail filtering software, assuming the CPU is powerful enough to perform the filtering. The increased traffic volume can be significant. AOL estimates that as much as 30% of its 30 million e-mail messages may be spam [19]. The additional cost to handle spam was estimated by one ISP, Netcom On-Line, to be at least $1 million per month, adding a minimum of an additional 10% to each subscriber's monthly bill [19]. Further, ISP customers may discontinue subscriptions as a result of the additional cost, the potentially slower Internet access, or the burden of sifting through large numbers of unsolicited messages [32]. Loss of customers is the major bottom line cost borne by ISPs. Dissatisfaction on the part of customers can prompt action.

III. Responses to Spam

A variety of measures have been undertaken to minimize the negative impacts of spam. Consumers and ISPs have undertaken initiatives to preclude spam from arriving and to contend with it once it has been delivered. The direct marketing industry has recognized the necessity to set standards for ethical and responsible distribution of commercial e-mail messages on the Internet. In addition, legislative action in the United States has been initiated at the

federal level and has been adopted in some states.

A. Responses by Consumers

Consumers themselves can employ a defensive strategy to minimize spam. The first line of defense is to not publish your e-mail address. Mass mailers acquire e-mail addresses from primary sources, such as forms requesting consumer information, and secondary sources, such as the purchase of subscriber, customer, or membership lists. Many forms now routinely ask for e-mail addresses purportedly for the purpose of completing a purchase, registration, application, or inquiry. Websites may require visitors to register before gaining entry. Admission may even be denied if the e-mail address provided cannot be validated, disallowing omission or use of fake addresses. Consumer use of e-mail for correspondence with a website is another means of collecting addresses. Attempts to be removed from an e-mail list by replying to spam may simply serve to confirm your address is actively used. Consumers may be unaware that their e-mail addresses are being collected. For example, computer programs known as "bots," short for robots, are designed to search the Internet for addresses. Users of Usenet, Internet interest groups, are particular targets of these search programs, which may peruse Usenet tables for e-mail addresses. This clandestine harvesting of e-mail addresses is also accomplished by accessing the servers of ISPs and other networks.

It has become more and more challenging for consumers not to provide their e-mail address. In response, consumers can utilize an e-mail service such as Lucent Technologies' Personalized Web Assistant. Available for free at www.lpwa.com, this proxy server will generate "target revocable e-mail." An endless supply of unique e-mail addresses, capable of being validated, are generated. Users may later discontinue an address should spam arrive. In e-mail correspondences, the return address can be removed from the e-mail header by deleting it or changing it through the options in the e-mail system. Alternatively, an anonymous e-mailer service, which performs as a gateway for e-mail, may be used. These services automatically remove all header information, including the address, and replace it with different information. For example, www.anonymizer.com will place a header which identifies anonymizer.com as the origin of the message. However, these measures impose a hidden cost in that consumers may not be able to access e-mail they desire to receive from legitimate sources.

No matter what cautions are taken, some junk e-mail is bound to get through, moving the line of defense to dealing with the unwanted messages. Filters may be used to scan e-mail received and discard or sort and organize messages in various ways. For example, messages from known spam addresses, such as cyberpromo.com, or with certain keywords in the message body, such as "xxx" or "sex," can be directed to the trash folder. Filters are not foolproof however, as they are ineffective against spammers who misrepresent their identity and against messages which contain a valid use of a keyword.

The potential to receive spam may be reduced, but not entirely eliminated, through care in supplying an e-mail address and through care in sending e-mail. Such caution may serve to minimize the potential for the address to be added to a spammer's list. If spam is nonetheless received, filtering may reduce the burden of sorting through messages. In both instances, reducing the potential for spam to be sent and sifting through spam received, the full burden still rests with the consumer.

B. Responses by Internet Service Providers

ISPs are responding to the increasing activity of spammers through acceptable use policies, cease and desist requests, blocking e-mail containing addresses of known spammers, equipping subscribers with filters, and through legal action. For example, TCG Cerfnet, a San Diego, CA, ISP amended its policy to include a ban on spam [30]. AOL CEO Steve Case has adopted an aggressive "block and tackle strategy" [12]. Although ineffective when spammers use false addresses, AOL intends to block as many spam e-mails as possible at its gateway and tackle spammers through both cease and desist letters and in court. AOL has been successful in obtaining restraining orders, injunctions, and settlement agreements against spammers [24]. Subscribers are also informed about unsolicited e-mail and are provided with software filters.

ISPs have filed lawsuits in response to both the use of their name as the originator of the spam and the use of their subscribers as recipients of spam. AOL, for example, has filed about 40 civil lawsuits under Virginia laws, its home state, primarily to block or limit spam [24]. Other ISPs, including CompuServe, Prodigy, and Concentric Network, have filed similar lawsuits. Additionally, several ISPs, such as Juno Online Services, have sought injunctions to prevent alleged forging of their electronic addresses on spam.

Corporate e-mail providers may decide to close off correspondence on the Internet to assure users receive no spam. Bell Atlantic Corp., for example, instituted tight security to eliminate all but approved e-mail [22]. Those authorized to correspond with the engineering staff are placed on a list, effectively excluding all others. This exclusion may, of course, apply to legitimate business mail, the price paid for exclusivity.

C. Industry Self-Regulation

In a report requested by the United States Federal Trade Commission (FTC), the Center for Democracy and Technology endorsed various solutions to reduce spam [11]. Among them are the use of software to filter unwanted messages and prohibiting spammers from using false identities. The DMA embraced the report and adopted new

rules which require their members to remove from e-mail lists those who have so requested. In the face of continued court decisions against spamming practices and proposed state and federal government regulations which could ban spam altogether or regulate spam activities, the DMA met with anti-spam advocates. The purpose was to formulate mutually agreeable recommendations for e-mail marketing and ways to jointly work toward reducing abuse by marketers. The resulting consensus recommendations include [21]:

- Support legislation which, at a minimum, prohibits false identification in commercial e-mail;
- Acknowledge opt-in as the most successful targeting method for online marketers (By "opt-in," the group agreed on the definition: "the recipient has stated and not rescinded his or her desire to receive the type of mail which you are sending.");
- Work to create a non-profit global opt-out list, supported by marketers and free to consumers, which offers both businesses and individuals a one-time global opt-out from unsolicited commercial bulk e-mail.

Some e-mail marketers have independently taken it upon themselves to act in a responsible manner. For example, five of the largest spammers voluntarily offered a proposal to the FTC [35]. The proposal included both the removal from their lists upon consumer request and the payment to service providers to cover the costs of message delivery. To ensure delivery only to willing recipients, NetCreations uses a double opt-in approach [20]. Consumers first sign up with NetCreations' website by selecting from among choices presented. An e-mail message is then sent, to which the consumer must reply, as a second confirmation of the desire to receive future messages.

IV. Legislative Action in the United States

The efforts of consumers, service providers, and spammers themselves all have shortcomings, resulting in a continuation of the spam challenge. A seemingly simple solution would be to ban spam through legislation. This is probably neither possible nor desirable. An outright ban is probably not possible because of the fundamental free speech protection of the First Amendment to the United States Constitution, nor would such a content-based restriction be desirable because of the issue of censorship.

The First Amendment of the United States Constitution states that "Congress shall make no law... abridging the freedom of speech, or of the press..." This prohibition applies to governmental action whether federal, state, or local. Although spam, as a form of commercial speech, would receive less protection than other forms of speech, it still is nevertheless protected. Restrictions based on content are disfavored by the courts [3].

A. Federal Legislation

Opponents of spam want its outright prohibition, as is the case for unsolicited commercial faxes. The nuisance of such faxes was effectively ended by the Telephone Consumer Protection Act of 1991. This act, banning unsolicited faxes containing advertisements, survived constitutional challenge because the prohibition was reasonably fit to protect the substantial government interest of preventing the shift of advertising costs to consumers [10]. For spam, is the cost shifting to ISPs and consumers sufficient to constitutionally permit an outright ban? Legal commentators think not [23]. Legislation prohibiting unsolicited commercial e-mail would probably be treated similar to the Communications Decency Act (CDA) of 1996 which prohibited the transmission of obscene, indecent and patently offensive material to minors. The CDA was held unconstitutional as an impermissible content based restriction on speech [28].

Several anti-spam bills have been proposed in Congress, as summarized in Table 1. The first is the Unsolicited Commercial Electronic Mail Choice Act of 1997, S. 771. This Act would require spammers to present "advertisement" as the first word in the subject line of any commercial e-mail. All routing information in the e-mail would be required to be valid. Further, the sender would be required to include their name, postal and e-mail addresses, and telephone number. The FTC may impose fines and penalties for violations. ISPs would not be held liable for spam, unless they created it. The Act also authorizes states and individuals to enforce sanctions under the Act.

The Netizen's Protection Act of 1997, H. R. 1748, would ban unsolicited, unwanted e-mail. The provisions of the Telephone Consumer Protection Act, which prohibits unsolicited fax, would be amended to prohibit unsolicited e-mail as well. This restriction is constitutionally questionable. Any other commercial e-mail sent would be required to contain the date and time the message was sent and the identity and return address of the sender.

The Electronic Mailbox Protection Act of 1997, S. 875, is unique in that a private cause of action is provided for the violation of any e-mail rules adopted by an Internet standards organization. E-mail sent from either a false or unregistered domain name or a disguised origination would be illegal. Spammers would be required to remove a recipient's name from the mailing list upon request. The sale, exchange, or harvesting of addresses would be prohibited.

The Data Privacy Act of 1997, H.R. 2368, focuses on certain individual electronic privacy issues, but also provides for the establishment of a computer interactive services industry working group to establish voluntary guidelines for spam. This legislation does not restrict or diminish spam directly. In fact, if industry friendly guidelines are established, the use of spam could actually increase.

Table 1. Pending Federal Legislation in the United States

Legislative Bill	Prohibit unsolicited e-mail	Enforce ISP's policies	Universal exclusion list	Honor opt-out requests	Sender ID/False headers	Require labels
Unsolicited Commercial Electronic Mail Choice Act of 1997 Sponsored by Sen. Murkowski Introduced 5/21/97 Status: pending in Senate	No	No	No	Yes	Yes	Yes
Netizen's Protection Act of 1997 Sponsored by Rep. C. Smith Introduced 5/22/97 Status: pending in House	Prohibit UCE	No	No	No	Yes	No
Electronic Mailbox Protection Act of 1997 Sponsored by Sen. Torricelli Introduced 6/11/97 Status: pending in Senate	No	Possibly	Possibly	Yes	Yes	No
Data Privacy Act of 1997 Sponsored by Rep. Tauzin Introduced 7/31/97 Status: pending in House	No	No	No	No	No	No
Anti-Slamming Amendments Act Amendments by Sens. Murkowski and Torricelli Introduced 2/9/98 Amended 5/12/98 Status: passed Senate	No	No	No	Yes	Yes	No
E-Mail User Protection Act of 1998 Sponsored by Rep. Cook Introduced 6/24/98 Status: pending in House	No	Yes	Possibly	Yes	Yes	No
Digital Jamming Act of 1998 Sponsored by Rep. Markey Introduced 6/25/98 Status: pending in House	No	Sender's ISP only	Yes	Yes	Yes	No
Inbox Privacy Act of 1999 Sponsored by Rep. Markey Introduced 3/25/99 Status: pending in House	No	Opt-out by ISP	No	Yes; also opt-in by ISP customer	Yes	Yes

Based on: John Marshall Law School, 1998

The Anti-slamming Amendments Act, S. 1618, would require the sender of an unsolicited commercial e-mail message to include at the beginning of the body of the message, the name, physical address, e-mail address, and telephone number of the sender or of the creator of the message's content. This provision of the Act also requires a statement that further transmissions of such mail to the recipient by the sender may be stopped at no cost to the recipient by sending a reply to the originating e-mail address with the word "remove" in the subject line. E-mail from the sender to that individual must then cease. The Act does not apply to an ISP unless it initiates the transmission or the transmission is not made to its own customers. Enforcement powers are given to the FTC, the states, and ISPs. This act passed the United States Senate and has been sent to the House of Representatives. It is the only federal anti-spamming legislation to have cleared at least one chamber of Congress.

Two anti-spamming bills were introduced in the House of Representatives within one day of each other. The E-mail User Protection Act of 1998, H.R. 4124, introduced June 24, 1998, and the Digital Jamming Act of 1998, H.R. 4176, introduced June 25, 1998. The E-Mail User Protection Act of 1998 is essentially a House version of the previously discussed Senate's Electronic Mailbox Protection Act of 1997. The primary difference is that the House Act clearly prohibits a knowing contravention of an ISP's rules with respect to unsolicited commercial e-mail messages. It provides relief for both individuals and ISPs. The Digital Jamming Act of 1998 focuses not just on spamming, but also on the unethical telecommunications practices of slamming and cramming. With respect to spamming, the Act authorizes the Federal Communications Commission (FCC) to promulgate regulations requiring ISPs to notify subscribers of the right to give or revoke an objection to receiving spam, and the manner in which such right may be exercised. This Act also contains disclosure and opt-out provisions.

Comprehensive anti-spamming legislation was recently introduced in the Senate on March 25, 1999. The Inbox Privacy Act of 1999, S. 759, includes the consumer protection

contained in the previously discussed bills. What is unique about this Act is that it allows a domain owner (ISP) to elect not to receive unsolicited commercial e-mail by setting up a domain wide opt-out system. Should the domain owner elect or opt-out, the Act requires notice to the customers who may then elect to opt-in if they so decide. Enforcement is authorized by the FTC, the states, and ISPs.

B. State Legislation

Spam is a national problem within the United States. Because of interstate commerce implications, the regulation of spam should be by federal legislation. Since the federal government has failed to act, many states have introduced anti-spam legislation based on a state's long-arm jurisdiction power. These bills range from the probably unconstitutional outright prohibition of spam to the more common identity and address disclosures, and recipient opt-out procedures common in the proposed federal bills. The need for disclosure and opt-out protection was supported by a study of AT&T and Lucent Technologies spam e-mail. The study found that only 36% of the spam contained instructions for being removed from the mailing list and fewer than 10% identified the name, postal address, telephone number, and e-mail address of the sender, as required by the DMA guidelines [9].

In addition to the above protection, two most recently enacted state bills have additional provisions. On March 29, 1999, Gov. Gilmore of Virginia signed into law seven legislative measures to regulate the Internet. Of particular interest is the criminalization of some spam practices, such as providing false message transmission information [36]. In 1998, California enacted legislation providing for disclosure and opt-out protection. However, this legislation enhanced consumer protection by requiring the subject line of unsolicited advertising e-mail to include ADV: as the first four characters. Further, if the advertisement or its subject matter "may only be viewed, purchased, rented, leased, or held in possession by an individual 18 years of age or older," then the subject line must include ADV:ADLT as the first eight characters [5].

State anti-spam legislation does not resolve the problem. It is piecemeal at best and possibly unconstitutional as a burden on interstate commerce. A legislative solution to the problem of spam must be enacted at the federal level by Congress. Such an act would preempt state law and establish a uniform national policy. As e-mail and online information become more prevalent, supplanting the more traditional channels of communication, federal legislation is likely to follow, as evinced by the pending legislation. While such legislation is certain to regulate spam, senders of spam may try to circumvent the law by simply routing their messages through overseas computer systems, or locating offshore, thereby attempting to shift jurisdiction. Legislation is unusually problematic in the special environment of cyberspace. Constitutional and jurisdictional litigation will surely commence after the passage of anti-spam legislation.

V. RECOMMENDATIONS

Public policy issues relative to spam are numerous. A number of these issues are not too far differentiated from similar issues relative to other media. Two issues appear to be unique to spam, jurisdictional domain and the transfer of costs. In response to these issues, three recommendations are presented.

A. Issues Similar to those of Other Media

The issues associated with spam which are similar to issues in other types of media should be addressed in like manner as has evolved through earlier public policy development. For example, questionable content is also a concern in direct mail, television advertising, and other media. Similarly, deception, privacy, and free speech concerns are issues with other forms of media.

B. Issues Unique to Spam

Spam is unique relative to two concerns previously identified, jurisdictional domain and the transfer of costs. First, the jurisdictional issue is more complicated given that cyberspace does not possess the same territorial boundaries, or, at a minimum, the same contract necessity to enter the media channel, as other marketing communication modalities. The jurisdictional question in its entirety is beyond the scope of this paper. At least within the United States, the federal level, in lieu of a currently viable global alternative, is proposed as the locus of legal boundary for legislative action. The jurisdictional issue is certain to continue to pose enforcement problems.

Second, the cost transfer concern does not exist with traditional media, but is a major issue with spam. Free markets require the flow of information to efficiently effect exchange. When information is restricted, markets will operate less efficiently. However, recent fragmentation of existing traditional marketing communication channels (more television channels, cable television, more magazines, and so forth) has increased the challenge for marketers who wish to disseminate information to existing or potential markets. E-mail has the potential to allow marketers to communicate very efficiently with targeted markets. The unique problem, unlike other media, is that spam costs are at least partially transferred to the targeted consumer and to the ISP, as discussed above. The public policy issue is how best to enable the free market system to utilize e-mail communications while at the same time protecting the consumer and ISP from “costs” which they have incurred, not of their own free will.

A ban on unsolicited e-mail has the potential to harm the efficiency of the free market process. However the converse, no limitation, unfairly transfers the cost to the e-mail recipient

who, if given the choice, may choose not to participate in the exchange process. The "opt-out" option, which appears to be the mechanism of choice in much of the proposed legislation, does not prevent the cost transfer until an active decision is made by the targeted recipient. Alternatively, consumers who opt-in do so of their own free will. This choice may be viewed as the result of a decision calculus wherein the opt-in consumer has concluded that the benefits of unsolicited e-mail outweigh the costs. That is, at a macro level, the set of opt-in consumers who decide that their gains from participating in a more efficient marketing communication system and its inherent efficiencies offer more benefits than costs.

The transfer of cost issue should be addressed with opt-in as the central control mechanism. Opt-out should remain indefinitely as an option to those consumers who have chosen to "opt-in." This preserves consumer free choice within the free market system while still allowing for the development of data bases, a source of competitive advantage for the marketer. The information exchange remains beneficial to both as a result of the potential cost efficiencies of e-mail as the medium of communication.

VI. Conclusion

If utilized ethically, that is by providing quality content which users have agreed to receive on an intermittent basis, e-mail marketing can effectively reach a target market, with personalized communication, at a cost lower than alternative media. The savings realized can be passed on to consumers through product discounts and special offerings. The potential for consumer benefit may outweigh the nuisance of a few unwanted messages. The challenge for today is that the marketers, government, ISPs, and consumers must contribute to the development of an internet marketing process that is consistent with free market principles.

References

[1] K.J. Andrews, "Opt-in e-mail," *Target Marketing*, February 1, 1999, Vol. 22, Iss. 2, pp. 105, 108.

[2] S. Bahr, "No stomach for spam," *America's Network*, December 1, 1998,Vol. 102, Iss. 23, p. 12.

[3] S.E. Bennett, "Canning spam: CompuServe, Inc. v. Cyber Promotions, Inc.," 32, *University of Richmond Law Review*, 545, March, 1998, p. 547-570.

[4] *Business Week*, "A little net privacy, please," http://www.businessweek.com/@@4WZJy4cASJ2SwAA/1998/11/b3569104.htm.

[5] *Cal. Bus. and Prof. Code* 17538.4, 1998.

[6] K.K. Campbell, "A net.conspiracy so immense... Chatting with Martha Siegel of the Internet's infamous Canter & Siegel. CuD 6.89, October 1, 1994, http://www.eff.org/pub/Legal/Cases/CanterSiegel/c-ands_summary.article.

[7] K. Carr, "Stamping out spamanoia," *CIO*, March 1, 1999, Vol. 12, Iss. 10, pp. 56-60.

[8] M. Castelluccio, "Spam and cheese?" *Management Accounting*, February, 1999, Vol. 80, Iss. 8, pp. 82-83.

[9] L.F. Cranor and B.A. LaMacchia, "Spam!" *Communications of the ACM*, August, 1998, Vol. 41, No. 8, WL 13668548, p. 74-83.

[10] *Destination Ventures, Ltd. v. FCC*, 46 F. 3d 54 (9th Cir. 1995).

[11] "Internet industry finds no solution to stop spam," *Direct Marketing*, September 1, 1998a, Vol. 61, No. 5, WL 13872570, p. not available.

[12] "The fight against spam," *Direct Marketing*, May 1, 1998b, Vol. 61, No. 1, WL 13872370, p. not available.

[13] *Direct Marketing Association*, http://www.the-dma.org/lobbypages/lobby-reception.html.

[14] E. Elliott, "News from the 81st Annual Conference: Wientzen surfs the web," *The DMA News*, http://www.the-dma.org/texis/scrip...hwBmWfeGwzwwwr/displayArticle.html.

[15] J. Erickson, "Are those who go online to send junk mail out of line?" *Star Tribune*, June 30, 1996, p. 3D.

[16] *FTC*, "FTC names its dirty dozen: 12 scams most likely to arrive via bulk email," July, 1998, http://www.ftc.gov/bcp/conline/pubs/alerts/doznalrt.htm.

[17] E.R. Foxman and P. Kilcoyne, "Information technology, marketing practice, and consumer privacy: Ethical issues," *Journal of Public Policy & Marketing*, Spring 1993, Volume 12, Number 1, start page 106.

[18] S. Godin, "A guest opinion: Permission key to successful marketing: Turning prospects into customers demands commitment from both," *Advertising Age*, November 10, 1997, WL 13675454, p. not available.

[19] D. Harper, "Hold the spam, please," *Industrial Distribution*, February, 1999, Vol. 88, Iss. 2, p. 98.

[20] J. Hu, "When is email marketing spam?" *Cnet News.Com*, August 31, 1998, http://www.news.com/News/Item/0,4,25891,00.html.

[21] C. LaMotta, "Anti-spam advocates and Direct Marketing Association meet to identify consensus recommendations for e-mail marketing," *The DMA News*, http://www.the-dma.org/texis/scrip...hwBmWeI7ncwwwr/displayArticle.html.

[22] S. Machlis, "Group issues advisory in memo that acknowledges spam as corporate evil," *Computerworld*, October 31, 1997, http://www2.computerworld.com/home/online9697.nsf/All/971031group19CDE.

[23] J.A. Marcus, 1998, 16 *Cardozo Arts and Entertainment Law Journal* 245.

[24] *The John Marshall Law School, Center for Information Technology & Privacy Law*, http://www.jmls.edu/cyber/index/spam.html, visited March 26, 1999.

[25] *The National Law Journal*, "SEC does a 'net sweep and charges 44," November 9, 1998, Volume 21, Number 11, p. A9.

[26] J. Postal, "On the junk mail problem," *Network Working Group Request for Comments*: 706, NIC #33861, November, 1975, ftp://ftp.internic.net/rfc/ rfc706 .txt.

[27] *Public Workshop on Consumer Privacy on the Global Information Infrastructure*, http://www.ftc.gov/bcp/conline/pubs, July 1966.

[28] *Reno v. ACLU*, 117 S. Ct. 2329 (1997).

[29] J.I. Richards, "Legal potholes on the information superhighway," *Journal of Public Policy & Marketing*, Fall 1997, Volume 16, Number 2, start page 319.

[30] P. Riedman, "Interactive: Juno sues over falsified addresses: Spam lawsuits begin to pile up," *Advertising Age*, December 1, 1997, WL 13675725, p. not available.

[31] A. Schwartz and S. Garfinkel, "Stopping spam," *O'Reilly & Associates, Inc*., October, 1998.

[32] S.A. Smith and E.W. Davis, "Is spam edible?" *CIO Web Business Magazine*, December 1, 1998, http://www.cio.com//archive/120198_gray. html.

[33] S. Stambler, "The future looks bright for e-mail marketing," *Marketing with Technology News*, August 28, 1998, Volume 7, Issue 12, http://www.mwt.com/aug98art.html.

[34] M. Stroh, "Spam is still the biggest irritant of e-mail," *The Baltimore Sun*, March 24, 1999, WL 5177613, p. 1A.

[35] I. Teinowitz, "E-mailers offer to trim 'spam,'" *Advertising Age*, June 16, 1997, WL 8287748, p. not available.

[36] *The Washington Post*, March 31, 1999, p. B4.

[37] K. Woo, "Making e-mail marketing work," *Target Marketing*, February 1, 1999, Volume 22, Issue 2, WL 11878745, p. not available.