Report to the Federal Trade Commission

of the

Ad-Hoc Working Group

on

Unsolicited Commercial Email

JULY 1998

FOREWORD

This document reflects the work of the Ad-Hoc Working Group on Unsolicited Commercial Email. The recommendations offered reflect the Working Group's efforts to reach consensus on appropriate first steps to address the problems associated with unsolicited commercial email (UCE). Many of the participants have additional views on UCE that are not encompassed in this report. The recommendations do not necessarily represent the views of the organizations with which the participants are associated. We encourage you to contact the participants to learn more about the issue and their position; a list of organizations, companies and individuals who participated in meetings is provided at the end of the report.

ACKNOWLEDGEMENTS

As the coordinator of the Ad-Hoc Working Group on Unsolicited Commercial Email and primary drafter of this report, I would like to thank all the participants for their tireless effort to listen to opposing points of view, express their own views clearly, grapple with complex technical and legal issues, and work to forge consensus where many thought none existed. I am especially grateful for: the technical expertise provided by Paul Hoffman and Lorrie Faith Cranor; the efforts of Roger Cochetti and Glee Cady to keep us focused on the big picture; the consumer-oriented focus brought by Ram Avrahami; and the thoughtful comments provided by Jill Lesser, Jim Halpert, Rachel Luxemburg, Ron Plesser and Ray Everett-Church. Finally, my thanks, and those of the participants, go out to CDT interns Zachary Brown, Jacob Remes, Ernest Miller, and Adam Scoville whose research, writing and editing made this report possible.

Deirdre K. Mulligan

INTRODUCTION

The Federal Trade Commission's June 1997 Workshop on Consumer Privacy marked the beginning of a focused discussion of the problems associated with unsolicited commercial email (UCE). The testimony and statistics presented to the FTC provided a basis from which to search for solutions to what most workshop participants, analysts, and email users have identified as a problem that is, at present, unlikely to be solved by market forces alone. Comments and presentations before the FTC detailed the independent and collective efforts, involving nearly every segment of the online population, to address the problems arising from unsolicited commercial email. [1]

The half-day workshop on unsolicited commercial email documented the frustrations of email users — both individuals and businesses — with the growing clutter of unsolicited messages in their in-boxes. It documented the growing burden that unsolicited commercial messages place on Internet service providers. It raised important questions about the future of email — will it be a useful medium for a variety of communications or will it be overrun by an onslaught of unsolicited, and often fraudulent, commercial messages?

Several areas of consensus emerged during the FTC's workshop.

- A desire to maximize individual email users' control over the information that enters their in-boxes. The majority of proposals put forth focused on providing individuals with the ability to gain more control over the range of commercial messages they receive.
- A desire to ensure that costs were not unfairly imposed upon end users, and Internet and online service providers.
- A desire for increased government action to combat fraudulent unsolicited commercial email. Participants welcomed increased enforcement of existing FTC regulations and state laws regarding unfair, deceptive and misleading commercial statements.
- A belief that, to date, technology, self-regulatory efforts and case-by-case legal action have had a limited impact on unsolicited commercial email.
- A desire to deal with the problems associated with unsolicited commercial email in ways that respect the First Amendment rights of Internet users and the speech enhancing potential of the Internet.

[1] The range of approaches includes seeking legal redress, establishing joint industry association guidelines to set parameters on appropriate behavior, providing user and ISP-based filtering tools, and various vigilante efforts. The complete record of comments submitted to the FTC about UCE can be found at <www.ftc.gov/bcp/privacy2/comments/>.

Most of the FTC workshop participants were focused on the cost shifting and intrusiveness of UCE, rather than on the commercial nature of the communication. While unsolicited commercial messages are currently the problem, several participants noted that the quantity of the messages, their unsolicited nature and the cost shifting were the source of complaints and problems independent of the content of the message. Participants recognized that proposed solutions to these content-independent problems may have First Amendment implications.

Most of the FTC participants supported rules — be they guidelines or legislation — requiring commercial messages to have accurate headers and domain names and to include accurate contact information within the text of the commercial message. Participants identified forged addresses and domain names as the source of innumerable problems, ranging from the system overloads caused by mis-routed replies to the damage caused to the reputation of individuals and companies when they are portrayed as the sender of UCE. Akin to requiring accurate return address information on postal mail, participants viewed accuracy as an important step in addressing the costs incurred by recipients of UCE.

Beyond the areas of fraud prevention and requiring "return address" accuracy, a diversity of proposals and views was presented to the FTC. Proposals ranged from extending existing models for addressing unsolicited commercial messages in other media, such as the Telephone Consumer Protection Act (banning unsolicited commercial faxes) and self-regulatory "opt-out" mechanisms for telephone and mail solicitations, to reliance on "filters" and other technical mechanisms to screen out and block unwanted email.

Despite the wide agreement on the nature of the problem, participants in the FTC forum did not unite around a single solution. However, at the urging of then-Commissioner Varney, participants agreed to undertake a collaborative effort to identify workable solutions to the problems arising from unsolicited commercial email.

Over a ten month period, under the coordination of the Center for Democracy and Technology (CDT), many participants in the FTC's workshop on unsolicited commercial email, joined by other interested parties, explored the issue of UCE, reviewed proposals and identified a range of potential solutions. The initial goal of CDT's Ad-Hoc Working Group on Unsolicited Commercial Email (Working Group) was to provide a venue for in-depth exploration of the problems initially identified at the FTC workshop. Participants in the Working Group agreed early on that developing workable solutions required a nuanced understanding of the technical aspects of the Internet and email, the impact of UCE on network operators and end users, the "harms" identified during the FTC workshop, and the legal and technical tools currently available to address UCE, as well as respect for First Amendment values. The Working Group was briefed by outside experts and fellow participants on a range of topics, including the workings of email and various email filtering programs, the prosecution of email fraud and the genesis of current legislative proposals. This process has enabled the Working Group to hone in on the key issues that must be addressed by any UCE solution.

This report documents the progress, findings and recommendations of the Working Group. The goal of the Working Group and this report is twofold. The report attempts to provide a factual basis for efforts to address UCE. The report begins by establishing the specific issues raised by UCE and then considers the extent to which the various legal, technical and self-regulatory approaches proposed to date address these issues. The analysis offers both a review of general approaches and, where appropriate, comments on specific proposals. Throughout its analysis, the Working Group attempted to identify other policy

considerations that should be considered in evaluating the feasibility and suitability of proposed solutions. In conclusion, the report puts forth a set of recommended actions that the Working Group as a whole believes should be taken in this area.

The report consists of five sections:

- **Section I** provides context by outlining the scope of the report, and discussing characteristics of the Internet relevant to the discussion of UCE.
- **Section II** outlines the impact on users and network operators of unsolicited commercial email.
- **Section III** surveys and analyzes the legal and technical tools available to address UCE.
- **Section IV** reviews and analyzes several key legal, technical and self-regulatory proposals under consideration to address UCE.
- **Section V** contains recommendations.

I. DEFINING THE PROBLEM IN CONTEXT

A. Unsolicited Commercial Email: what this report is and is not about.

The focus of this report is unsolicited commercial email. While recognizing that many of the issues associated with UCE arise due to its unsolicited and bulk qualities and not its commercial content, the Working Groups' focus has been on UCE for two reasons: the majority of unsolicited email messages today are commercial; and focusing on UCE allowed the Group to steer clear of the legal issues associated with other forms of speech, such as unsolicited political email messages.

While informal estimates indicate that today roughly half of unsolicited commercial email messages contain fraudulent or deceptive content, the other half containing truthful commercial messages also raise issues that need to be addressed. There are laws on the books to combat fraud, regardless of whether it is conducted through the mail, over the phone, or on the Internet. Non-fraudulent UCE messages are a more complex issue, and they are a focus of this report. On the one hand, such messages are truthful speech protected in the United States like other speech, albeit less strongly, by the First Amendment. On the other hand, messages that are truthful in content, but include intentionally inaccurate email header information, make up a very large volume of Internet traffic and unwanted messages in end users' mailboxes today. A new wrinkle emerges from the events of recent months that reveal many of the issues associated with UCE arise when companies or organizations send unsolicited email in bulk regardless of its content. [2]

The issue and the solutions ultimately chosen to address UCE touch on core civil liberties concerns and have ramifications for the future of the Internet. UCE-oriented policies could have a negative impact on online speech and individual privacy or other unintended consequences for the Internet.

B. The Internet Environment

Implementing policy in a global, networked environment presents a series of challenges. Effective responses to UCE in international networks must respond to several considerations: the increased generation and collection of information by a growing number of entities, the ease of crossing national borders, and the lack of centralized control mechanisms.

[2] The political organization Informed Voter is using email to contact potential Democratic voters. In response to criticism, Robert Barnes, a principle in the firm, agreed that he was "just trying to leverage one of the most powerful mass media available today to reach voters who would want to be contacted." Janet Kornblum, Political Mailings Criticized As Spam, CNET NEWS.COM (April 22, 1998) <http://www.news.com/news/item/0,4,21376,00.html>; and Carla Marinucci, Candidates Canvassing By E-Mail: State Democrats Harness Technology, SAN FRANCISCO CHRON. (April 18, 1998) <http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/1998/04/18/mn13037.dtl>.

1. The ease of expressing ideas and sharing information.

Email is a powerful medium for expressing ideas, supporting commerce, sharing opinions, and receiving information. As the Supreme Court decision Reno v. ACLU [3] recognized, the Internet offers new opportunities to maximize individuals' ability to choose the opinions and ideas worthy of attention and adherence. Across the globe, email is spanning distances and cultures by facilitating the exchange of knowledge, ideas, opinions, products and services. Email is an inexpensive way for advocates, activists and marketers to spread "the word," whatever it may be. The breadth of information and opinions available, the ability to communicate en-masse, as well as one-to-one, and the speed with which information can be disseminated, views expressed and appropriate action prompted (if they can be harnessed) bode well for a more informed, active and concerned body politic in the 21st Century. Commercial messages and commercial solicitations can play an important role in informed consumer choices and commerce. However, the unbridled use of email for unsolicited commercial messages may hamper both the Internet's commercial potential and undermine the very First Amendment values that enable UCE. Sobering evidence of the damage that can result is provided by numerous news groups that have grown silent due to the influx of UCE and the harvesting of participants' email addresses.

2. Low barriers to access.

As the Internet and the World Wide Web expand to become a major international means of communication and commerce, use of email to communicate about social, political and commercial activities will increase. The availability of low-cost trial, even free, email accounts allows some individuals to engage in email marketing at virtually no cost. As structured today, email can offer a method of disseminating one's opinion or commercial message nearly devoid of start-up costs compared to other forms of direct communication, such as telephone and mail. In addition, the availability of email addresses, which can be purchased or "harvested" using email trolling programs from postings and online chat areas, greatly facilitate UCE. The relative lack of access barriers is a great strength of the Internet; however, it also aids those engaged in the practice of sending unsolicited bulk messages (commercial or other). When considering programs aimed at UCE, every effort should be made to preserve the open environment that gives the Internet so much of its vibrancy. Solutions should also be examined for the disparate impact that they may have on smaller and start-up companies in comparison to large, established companies.

3. The ease of crossing national borders.

In a global network environment, information crosses national borders and individuals interact with entities outside national borders with great ease. The Internet allows information, including email, to flow quickly and seamlessly from one nation to the next without passing through checkpoints and permits individuals to interact with entities outside national borders. National laws may be insufficient, on their own, to provide citizens with relief from UCE due to the global nature of the medium. As many have said, the global nature of the Internet may drastically limit the effectiveness of policy decisions, unless they reflect broad consensus and are implemented and enforced in a fashion that addresses the Internet's characteristics.

[3] 117 S. Ct. 2329 (1997).

4. The lack of centralized control mechanisms.

Unlike many communications systems, the Internet does not have central points of control. The decentralized nature of the Internet allows it to cope with problems and failures in any given computer network by simply routing in another direction. This makes the Internet quite robust. However, the lack of readily available centralized control mechanisms may frustrate those seeking to regulate activities on the network. [4] Sometimes a rogue action or policy of a single computer network can cripple a collective effort at governance. Broad agreement on goals, and coordinated action, are necessary to deal effectively with pressing Internet issues.

5. The ability to place individuals' in control of their network interactions.

Client-side controls present new opportunities to empower individuals. The Internet continues to shift control over interactions away from the government and large private sector companies. The ability to build protections — against UCE, other objectionable content, or for privacy — into the user interface with the network offers the opportunity to allow individuals to craft protections that shield them regardless of the jurisdictional law and policy. Providing individuals with the technical means to control email may pave the way for protections that are as decentralized and ubiquitous as the networks themselves. Such tools place individuals, rather than network operators or governments, in a position to decide which incoming email messages are acceptable.

Developing methods of implementing and enforcing policies that respond to the decentralized, global and borderless nature of international networks is essential. Additional technological solutions and efforts at self-governance may be valuable supplements to the traditional top-down methods of implementing policy and controlling behavior (e.g., international agreements, national legislation, or self-regulatory codes of conduct) which may offer incomplete responses to the issue of UCE in the global information infrastructure. While finding consensus on appropriate policy is a first step, in a networked environment structuring effective implementation becomes nearly as complex as reaching policy consensus. Effective monitoring on this vast scale may tax the resources of those responsible for enforcing policies — be they international bodies, state and local governments or trade associations.

Addressing the flow of UCE along this international network may require new tools for implementing policy. For this reason, those seeking solutions to the problems associated with UCE have examined the ability of law, self-regulation and technology, independently and in consort, to address this issue.

[4] Attempts to regulate the availability of encryption on the Internet highlight the frustrations that regulators may experience. As many scholars and advocates have pointed out, national attempts to restrict the availability of encryption are likely to be ineffective. For if even one jurisdiction (or one network in one jurisdiction) fails to restrict encryption, individuals world wide will be able to access it over the Internet and use it.

II. ISSUES RAISED BY UNSOLICITED COMMERCIAL EMAIL

Internet users, Internet Service providers ("ISPs" or "service providers") and, most recently, policy-makers have identified unsolicited commercial email, particularly when sent in bulk, as a problem of serious consequence for the Internet. Although complaints about unsolicited commercial email differ from users to ISPs to network providers, there has been an effort to identify the issues that any effective UCE-oriented policy must address. These issues grow out of the adverse consequences of UCE. The harms commonly identified by users and ISPs as stemming from the influx of unsolicited email fall in three broad categories: invasion of individual privacy; unfair cost shifting; [5] and misappropriation of facilities.

A. Impact on users

The primary issues raised by unsolicited commercial email voiced by Internet users are that:

- it intrudes upon individual privacy;
- identifying and deleting unwanted messages places a burden on the individual's limited time; and,
- it inappropriately imposes costs on individuals in the form of connection time and server and disk storage space among others. [6]

These complaints can be separated into three general categories of concern:

- **Privacy concerns** — from where did they get my email address, why are they intruding into my home?

The privacy interests [7] of recipients of unsolicited commercial solicitations have motivated both federal and some state governments to enact limits on such communications in media ranging from face-to-face communications (door-to-door solicitations), [8] postal mail, [9] telephone, [10] and facsimile. [11] In the U.S., privacy is protected through a loose framework of statutes, common law actions, and industry codes of conduct. Many of the laws and regulations limiting unsolicited communications have

[5] EF-Austin, EF-Florida, and Voters Telecommunications Watch, Comments to the Federal Trade Commission on Unsolicited Commercial Email, June 2, 1997. The cost issues addressed in this section are largely taken from these comments, by permission.

[6] Based on an informal survey of 11 ISPs' expenses related to UCE. As much as $2 of a monthly service bill may be attributed to UCE. Daniel P. Dern, Spam Costs Internet Millions Every Month, CMP NET,(May 4, 1998) <http://pubs.cmpnet.com/telepath/21new2.htm>.

[7] On the state's interest in protecting privacy, see: Florida Bar v. Went For It, Inc., 515 U.S. 618 (1995) (upholding temporal ban on direct mail solicitation by personal injury lawyers). "[A] special benefit of the privacy all citizens enjoy within their own walls, which the State may legislate to protect, is an ability to avoid intrusions." Id. at 625 (citations omitted); Rowan v. Post Office Dept., 397 U.S. 728, 736-37 (1970) (upholding postal regulation of offensive mail).

been the subject of litigation. The privacy of recipients has been found to support some limits on unsolicited commercial solicitations, but the First Amendment rights of both commercial speakers to communicate and of individuals wishing to receive such solicitations have led courts to find differing levels of regulation permissible depending upon the characteristics of the medium. In reviewing restrictions, courts have paid special attention to the amount of control individuals can exercise over content, the medium's invasive nature, [12] and to other harms claimed by the unwilling recipient, such as the ability of the medium to shift costs onto the recipient or its interference with the individual's ability to receive desired communications. [13]

Similar to the discussions and debates surrounding other forms of unsolicited marketing, unsolicited commercial email has at times been met with complaints by individuals who object to receiving unsolicited and

[8] Numerous state and local laws govern door-to-door solicitations. The U.S. Supreme Court has recognized both the legitimate privacy interests of individuals and the role that door-to-door communication plays in inexpensively disseminating ideas. Martin v. Struthers, 319 U.S. 141, 145-46 (1943). The Court has held that door-to-door solicitations can be governed by time, place, and manner restrictions but not banned. Id. at 149. But see, Breard v. Alexandria, 341 U.S. 622 (1951) (Unsolicited commercial door-to-door solicitation ban upheld). The Court has held that commercial speech could be subject to stricter controls. Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557, 564-65 (1980). However, more recent decisions have emphasized the First Amendment protections of truthful and non-misleading commercial speech. See, 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484 (1996); City of Cincinnati v. Discovery Network, Inc., 507 U.S. 410 (1993).

[9] Interestingly, a number of proposals currently under consideration by Congress attempt to address the problem of direct mail by limiting the sale and rental of personal information by entities who collect it. See, Personal Information Privacy Act of 1997, S. 600, 105th Cong. (1997) (introduced by Sen. Feinstein); H.R. 98, 105th Cong. (1997) (introduced by Rep. Vento); and, H.R. 1287, 105th Cong. (1997) (introduced by Rep. Franks). Other proposals aimed at limiting direct mail have focused on limiting the mail itself.

[10] See, Telephone Consumer Protection Act (TCPA) of 1991, 47 U.S.C. § 227 (1994).

[11] Id. The TCPA prohibits unsolicited facsimiles that contain advertisements. 47 U.S.C. § 227(b)(1)(C) (1994).

[12] Cf. Bolger v. Youngs Drug Products Corp., 463 U.S. 60 (1983), finding that, "the short, though regular journeys from mail box to trash can . . . is an acceptable burden (on individual privacy) . . . so far as the Constitution is concerned." Id. at 72 (citation omitted); State by Humphrey v. Casino Marketing Group, 491 N.W.2d 882 (Minn. 1992), cert. denied, 507 U.S. 1006 (1993), holding that "the residential telephone is uniquely intrusive. The caller . . . is able to enter the home for expressive purposes without contending with such barriers as time or distance, doors or fences. . . . Unlike the unsolicited bulk mail advertisement found in the mail collected at the resident's leisure, the ring of the telephone mandates prompt response, interrupting a meal, a restful soak in the bathtub, even intruding on the intimacy of the bedroom." Id. at 888.

[13] The report accompanying the TCPA details additional costs associated with automatic dialing systems. Findings include:
* automated calls are placed to lines reserved for emergency purposes, such as hospitals and fire and police stations; . . .
* the automated calls fill the entire tape of an answering machine, preventing other callers from leaving messages;
* the automated calls will not disconnect the line for a long time after the called party hangs up the phone, thereby preventing the called party from placing his or her own calls;
* automated calls do not respond to human voice commands to disconnect the phone, especially in times of emergency;
* some automatic dialers will dial numbers in sequence, thereby tying up all the lines of a business and preventing any outgoing calls; and
* unsolicited calls placed to fax machines, and cellular or paging telephone numbers often impose a cost on the called party . . . .
S.Rep. No. 102-178, reprinted in 1991 U.S.C.C.A.N. at 1969.

unwanted communications, frequently at their own expense. UCE containing messages or "pointers" to Web sites that contain information that is considered offensive, particularly information and images that parents consider inappropriate for their children, appears to be on the rise. Such UCE raises additional privacy concerns as it undermines parents' ability to protect their children from content they deem inappropriate.

- **Opportunity costs** — measurable by loss of productivity, where the dedication of resources to dealing with unsolicited commercial email interferes with the ability of the individual to engage in another task.

By far the soft costs most frequently cited by email users are the diversion of time and loss of productivity due to unsolicited commercial email. Depending on the effectiveness of filtering techniques and the email package employed by an individual or business, unsolicited commercial email can take anywhere from no time to several minutes to deal with. In considering the soft costs attendant to unsolicited email, a number of additional factors must be included in the calculus beyond the simple act of deleting unsolicited commercial email. For example, users who download their email to a remote computer instead of reading it at the service provider "waste" additional time during the download of unsolicited commercial email. Similarly, time taken to respond to and unsubscribe from email lists in order to avoid future mail, or to report unsolicited commercial email to an ISP, where it is in violation of a term of service, can be significant. Finally, as it is likely that unsolicited commercial solicitations are a contributing factor in many recent slowdowns of Internet email, a significant soft cost is the interference with timely receipt of wanted material (see service providers section below).

- **Hard costs** — measurable in dollars of resources, access fees, or storage costs. [14]

Given that those who do not wish to receive UCE outnumber those who do by a very wide margin, the net hard costs to end users should be considered as well. Hard costs vary tremendously, depending upon the Internet connection, pricing scheme, email program and other variables of the email connection of the uninterested end user. For some Internet users, online access is not a free, flat-rate telephone call. For those users, the meter is ticking when they are downloading, reading, or even deleting without reading, unsolicited commercial email. For businesses that use email, the cost of processing UCE through internal mail systems can be quite high.

There has been much discussion in the market about the pricing of Internet access. With some ISPs, the amount of time a user is connected to the system is metered. Even at a low rate, reading and deleting unsolicited commercial email costs the user money. In some localities, connect time can be quite expensive. [15] In areas of the country that lack high speed access due to poor telecommunications connections, the additional time spent downloading UCE can add up quickly. On the flip side, many larger ISPs have begun offering, and users have embraced, flat-rate pricing. Flat-rate pricing avoids imposing the cost of UCE directly on users. However, flat-rate pricing may still reflect the additional cost of UCE to the service

[14] EF-Austin, EF-Florida, and Voters Telecommunications Watch, Comments to the Federal Trade Commission on Unsolicited Commercial Email, June 2, 1997. Over 2,700 people answered the user survey, and 60 ISPs answered the institutional survey conducted for the Workshop.

[15] Joe Keely of Senator Frank Murkowski's (R-AK) office reported many complaints about the cost of unsolicited commercial email due to the expense of connect time in the state of Alaska (as high as $6 per hour). The VTW survey received varied answers for what connect time costs users, ranging from $0.50 to $4 per hour.

provider. Despite the move to flat-rate pricing by some service providers, many email users do not have unlimited access accounts and others must place a long distance call to retrieve email. Finally, although it is not a major part of the pricing model today, some users are charged on a per-megabyte basis for email stored at their service provider's site before it is read. [16]

B. Impact on ISPs

ISPs enjoy no benefit whatsoever from UCE and they do incur significant costs from it. This has led to vocal objections by many ISPs to UCE. Service providers' complaints are varied. Similar to users' concerns, unsolicited commercial email raises both "opportunity costs" and "hard infrastructure costs" for ISPs. Service providers' soft costs include the cost of network bandwidth and processing email. Costs such as staff time and storage can be categorized as hard costs. In addition, ISPs, particularly commercial online service providers, can incur a third cost that can be loosely described as damage to reputation or customer relations.

- **Opportunity costs**

ISPs pay for their Internet connectivity, usually in a "maximum capacity" fashion. The growth of a service provider's traffic load may require an upgrade of connectivity to handle the load adequately. So, while a particular message, or mass emailing, may not trigger a cost to the service provider, the traffic increase may lead to a significant cost. [17]

- **Hard costs**

Hard costs to ISPs include staffing, storage and phone line availability. Unsolicited email forces ISPs to incur additional staff costs, since many customers want to report unsolicited email. Surges of system activity caused by large influxes of unsolicited commercial email can cause disks to fill up and mail to stop working until it is attended to by a staff member. ISPs typically store email until customers pick it up. This cost is either borne by the service provider or passed on to the user.

[16] The range of responses stated that this cost is approximately $1 per megabyte.

[17] Informal survey findings reported in CMP NET reveal a range of expenditures and a range of costs. Dern, supra note 6. Sample responses:

> MindSpring Enterprises Inc., Atlanta: Twenty to 25 percent of the incoming email at this midsize ISP is spam, said Harry Smoak, MindSpring's director of Net abuse and terms of service policy. To support Usenet activity, MindSpring currently has about $500,000 in equipment. "If there was no spam, we could probably do with one-third to one-half this equipment," Mr. Smoak said. E-mail and Usenet spam consume about one to two T1s (1.5 megabits per second to 3 Mbps) of bandwidth between MindSpring and its upstream Internet backbone. Also used up is the time spent byone-and-a-half engineers on spam-related abuse issues.
>
> Erols Internet Services, Springfield, Va.: This midsize ISP spends $75,000 in salaries for three full-time employees whose sole responsibility is to deal with email abuse issues. "I would say it's among the reasons we recently had to up our prices," said an Erols system administrator. "Fully 10 percent to 15 percent of our e-mail disk space is taken up by incoming spam sent to Erols' customers. I estimate that probably five percent of the total traffic through Erols' networks is spam being bounced off our servers onto the rest of the Internet."
>
> GTE Internetworking, Cambridge, Mass.: "There are typically two to four people working full time on spam," said a spokeswoman at this ISP. "GTE has to deal both with spammers and spam itself."
>
> America Online Inc., Dulles, Va.: Of the average of 14 million email messages coming from the Internet to AOL daily, five to 30 percent are spam, an AOL spokeswoman said. "We have to scale the network to handle this," she said. "This costs the members, especially those who pay hourly rates." She declined to elaborate.

On systems where customers are encouraged to dialup, download their email quickly and disconnect, large amounts of unsolicited commercial email cause users to tie up dialup lines, thereby requiring ISPs to install more dial up facilities. Although ISPs do not currently pay per-minute costs on incoming calls from subscribers, they do need to ensure they have enough telephone lines, ports and modems to support their users. The longer users spend online downloading unsolicited commercial email, the more of these facilities ISPs need to purchase if they are to avoid a degradation in their quality of service.

- **Damage to reputation**

The reputation of a service provider can be damaged by outages, the use of falsified return addresses and domain names by senders of UCE that result in the ISP being blamed for or affiliated with it, and delays in service caused by incoming UCE. They can often be blamed for unwanted UCE when the sender inaccurately puts the ISP's name in the solicitation. Many ISPs have reported that heavy loads of UCE have delayed or prevented other, non-UCE email from getting through to their users. In addition to effecting the service provider's relationship with its customers, this may also lead to hard costs, such as new equipment purchases.

C. Impact on the Internet

Many users, ISPs and others are concerned that unsolicited commercial email is undermining the viability and usefulness of email as a communication tool. The variety of organizations, associations, companies and independent Internet users who are voicing concern, crafting guidelines, developing filtering or other anti-UCE devices, implementing filters and looking for possible legislative solutions is a strong indication that many on the Internet see unchecked unsolicited commercial email as a potentially corrosive force. Direct harms to the Internet can range from outages and crashes, due to overloads caused by bulk emailings, to problems caused by misdirected replies, to inaccurately addressed messages. The indirect harms caused by unsolicited commercial email are more diverse. Due to problems with unsolicited commercial email, some ISPs have chosen to cease participating in cooperative pass-through agreements, interfering with the flow of information across the proprietary networks that comprise a growing portion of the Internet.

The most dangerous, if least easily quantified cost, is the damage that unsolicited commercial email can cause to the reputation of email. The crashes, delays, lost messages and other problems causally related to unsolicited commercial email may well undermine the public's willingness to embrace this communication device for a range of functions that require a high degree of predictability and reliability. In addition, UCE can have a chilling effect on individuals' speech in that individuals may be reluctant to participate in online forums and Usenet groups, or may remove their email addresses from home pages for fear of getting their email addresses placed on mailing lists for UCE.

In response to UCE, some service providers have taken to limiting and blocking email from various domains. A loose consortium of service providers rejects all incoming email from a shared "black list" of "spammer-friendly" service providers. Some of the service providers who find themselves on the black list actually prohibit "spamming" in their terms of service, but because senders of UCE have taken advantage of their computers to "bounce" and "relay" messages, they have been targeted as part of the problem. As a result, the openness of the Internet is being undermined and the exchange of ideas is being diminished.

Internally, service providers' rules may take even higher tolls on speech. Many service providers' terms of services limit the sending of "spam" by subscribers. The definition of "spam" often hinges on the bulk nature of the message. In practice, this has limited not only unsolicited bulk commercial email messages, but all bulk mailings, regardless of how valuable they might be, including political and social messages. The Constitution provides greater protection to political speech than it does to commercial speech. In the long run such policies may negatively impact on a wide range of speech. Without examining the content of the messages — which would infringe on privacy — service providers are limited to using imperfect measures such as the bulk nature of a mailing in efforts to identify and eliminate unsolicited commercial email messages.

III. TOOLS CURRENTLY AVAILABLE TO ADDRESS UCE

A. Legal

In considering the law's role in combating UCE, it is helpful to divide UCE into two categories, UCE that contains fraudulent claims, and UCE that does not. Garden variety fraud that is conducted through email falls directly under existing law. Technical fraud, on the other hand, is defined as the variety of practices, such as relaying through third-party mail servers, dynamically forging header information and registering false domain names, used by those sending UCE to avoid detection, frustrate remove requests, misdirect replies, and generally frustrate efforts by users to prevent their continued receipt of UCE from the same sender. Unlike UCE that contains fraudulent claims, consumer protection laws may or may not reach technical fraud. Some service providers have successfully pursued other avenues in litigating against technical fraud.

Federal law empowers the Federal Trade Commission (FTC) and the Department of Justice (DOJ) to combat consumer fraud. In addition, the Computer Fraud and Abuse Act provides the federal government with statutory authority to investigate and prosecute those involved in damaging computers or accessing them without authorization. Under Section 5 of the Federal Trade Commission Act, the FTC can prosecute those engaged in deceptive or misleading trade practices. The Consumer Fraud Division of the Justice Department is responsible for protecting consumers against fraudulent business practices, regardless of the medium. Similarly, states have civil and criminal laws designed to protect consumers from fraudulent advertising and business practices. [18]

In February 1998, the FTC, in conjunction with the U.S. Postal Inspection Service, sent letters to more than 1,000 senders of fraudulent UCE. The agencies had examined emails submitted by consumers and identified those that appeared to be deceptive or fraudulent and in violation of the FTC Act or the Postal Lottery Statute. Letters were sent to the senders of the fraudulent UCE warning them that their activities might violate the law. [19] In March of the same year, the FTC filed its first action against a sender of UCE. [20] The FTC's complaint claimed that both the UCE and the homepage of Internet Business Broadcasting, Inc. contained false and misleading claims. The FTC

[18] See generally, People v. Lipsitz, 663 N.Y.S.2d 468, (N.Y. Sup. Ct. 1997). The New York State Court held that the state attorney general can pursue senders of UCE who violate consumer protection statutes. The defense argued that only federal courts could exercise jurisdiction in such matters. Lipsitz was enjoined from sending UCE advertisements, and ordered to pay restitution to the consumers whom he and his company had defrauded.

[19] Federal Trade Commission, FTC to Junk E-mailers: "No Scamming While You're Spamming" (Feb. 5, 1998) <http://www.ftc.gov/opa/9802/junk.htm>.

[20] Complaint for permanent injunction and other equitable relief, FTC v. Maher, et al. (visited June 25, 1998) <http://www.ftc.gov/os/9803/complain.htm>.

continues to monitor UCE. The FTC's complaint mailbox receives approximately 1,000 to 1,500 UCE messages from consumers daily. [21]

While the FTC and DOJ's Consumer Protection Division, as well as the states, are well armed to attack the problem of UCE that contains fraudulent and deceptive advertising within the body of the message (an enormous amount of UCE is likely to fit this definition), they have yet to take aim at UCE that, while containing truthful statements within the text, uses falsified header information to deceive end users into opening it. It appears that whether or not a forged header rises to the level of a deceptive practice for the FTC requires a case-by-case analysis. [22] If the body of an email message is non-deceptive, but the "from" line, "subject" line or "message header" is false the analysis would turn on whether a reasonable consumer is likely to rely on the false statement to her detriment. If, for example, a false "subject" or "from" line increases the likelihood that a consumer will download or read the message, and cost is incurred, there may be grounds to find the misrepresentation deceptive under Section 5 of the FTC Act.

Header information is viewed (if at all) only after a message is downloaded. Proving consumer deception based on a forged header, where the content of the message and the addressing information revealed to the message recipient are truthful, presents the most difficult scenario for a finding of deception. Even if the consumer views the header, it is possible that any inaccuracies are outweighed by the truthful information contained in the rest of the message. For these reasons, proving that the consumer relied upon the false header to her detriment may prove exceedingly difficult.

In any event, proving consumer deception and fraud based on addressing and header information is more complex than taking aim at the pyramid and get rich quick schemes that proliferate through UCE. Until law enforcement authorities (the FTC, DOJ or a state agency) brings successful prosecutions against senders of UCE for using falsified addressing information and falsified headers to deceive consumers, the legality of the use of intentionally false header information will remain unclear.

To clarify this issue, the state of Washington recently enacted a law, updating its consumer protection act, to prohibit explicitly the use of a third party's domain name, the misrepresentation of message origin, and the use of a false or misleading subject line in commercial email messages. [23] While it is not clear how successfully the state will be able to assert jurisdiction over most email, [24] this statute does

[21] The FTC maintains the address uce@ftc.gov for this purpose. The Junkemail.org Web site contains a questionnaire designed to aid consumers in identifying fraudulent UCE and sending it to the FTC. <http://www.junkemail.org>. The National Fraud Information Center also handles complaints about UCE. <http://www.nfic.org>.

[22] The content of this paragraph and the following paragraph have been checked with the Federal Trade Commission staff and they consider it to be an accurate statement.

[23] 1998 Wa. ALS 149; 1998 Wa. Ch. 149; 1997 Wa. HB 2752. The statute also creates the Select Task Force on Commercial Electronic Mail Messages. The task force is directed to identify technical, legal, and cost issues in relation to the transmission and receipt of commercial electronic mail messages, evaluate the sufficiency of existing laws, review efforts of the federal and other state governments, and prepare a report identifying policy options and recommend legislation if needed.

[24] State regulations that unduly burden interstate commerce are unconstitutional under the so-called "dormant" commerce clause. See, e.g., Kassel v. Consolidated Freightways Corp. of Del., 450 U.S. 662 (1981). A New York District Court has held that broad regulation of the Internet by a state is unconstitutional under this standard. ALA v. Pataki, No. 97 Civ. 0222 (S.D.N.Y. June 20, 1997) (order granting preliminary injunction).

provide clear guidance to the state's consumer protection agency, and puts senders of UCE on notice that accuracy in headers is required in the state of Washington. The prescriptive nature of the accuracy requirement will hopefully prod senders of UCE to follow appropriate Internet protocols, and will enhance service providers' and end users' ability to filter out unwanted messages, respond to those who send them unwanted messages, and take the cost of dealing with replies off the plate of innocent service providers and businesses and place them squarely on the sender of the messages.

The ambiguity over the legality of intentionally falsified email headers, and their damaging effect, suggests that a more proactive policy establishing accuracy requirements should be explored at the federal level. [25]

While consumer protection laws may or may not provide relief from technical fraud, the courts have granted service providers protection on other grounds. [26] The allegations contained in complaints filed by service providers range from violations of the Federal Computer Fraud and Abuse Act and various consumer protection statutes to common law trespass and conversion claims. Federal statutes protecting against wire and computer fraud [27] and racketeering [28] may offer avenues of relief. These federal statutes and similar state statutes have been cited to support plaintiffs' claims against the senders of unsolicited commercial email. In addition to criminal causes of action, service providers have claimed violations of various state laws forbidding deceptive trade practices. [29]

Trespass violations are the most common basis for anti-UCE lawsuits by ISPs. [30] Several lower and appellate courts have granted service providers relief, holding that the act of relaying UCE through proprietary computer networks — which often involves forging header information — constitutes a trespass.

Fitting UCE neatly into existing law can be complicated. The Computer Fraud and Abuse Act was designed to

[25] Without accuracy it is difficult to track down and identify those engaged in online commercial fraud, it is extremely difficult for service providers and users to filter out mail from unwanted senders, and it is nearly impossible for besieged end users to tell senders of UCE to remove them from their list. Accuracy requirements need not run afoul of the First Amendment protections for anonymous speech. Most anonymous remailers forbid the use of their services for UCE and accurately identify the source of the message as an anonymous individual. These services are infrequently used by senders of UCE.

[26] Companies and individuals whose domain names and addresses have been used by senders of UCE have also found relief through litigation. See, Parker v. C.N. Enterprises, No. 97-06273 (Tex. Travis County Dist. Ct. Nov 10, 1997) (visited June 26, 1998) <http://www.jmls.edu/cyber/cases/flowers3.html> (ordering injunctive relief and damages against a sender of UCE for using the plaintiff's domain name, "flowers.com").

[27] See, 18 U.S.C. § 1343 (1997); and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1997). Analysis is available courtesy of the Justice Department's Computer Crime and Intellectual Property Section (CCIP). Computer Crime and Intellectual Property Section, U.S. Dept. of Justice, National Information Infrastructure Protection Act of 1996: Legislative Analysis (last modified June 20, 1997) <http://www.usdoj.gov/criminal/cybercrime/1030_anal.html>.

[28] 18 U.S.C. § 1962(c) (1997).

[29] E.g. false, deceptive or misleading advertising. See, VA. CODE ANN. § 18.2-178 (1997) (criminal) and VA. CODE ANN. § 59.1-200A(8) (1997) (civil); and CAL. BUS. & PROF. CODE § 17500 (criminal) and CAL. BUS. & PROF. CODE § 321 (civil).

[30] See, Cyber Promotions, Inc. v. America Online, 948 F. Supp 456 (E.D. Pa 1996) (visited June 26, 1998) <http://www.jmls.edu/cyber/cases/aol-cp2.html>; Compuserve, Inc. v. Cyber Promotions, Inc., No. C2-96-1070 (S.D. Ohio May 7, 1997) (visited June 26, 1998) <http://www.jmls.edu/cyber/cases/cs-cp3.html> (final consent order by stipulation); Concentric Network Corp. v. Wallace, No. C-96 20829-RMW(EAI) (N.D. Cal. Nov. 5, 1996) (visited June 26, 1998) <http://www.jmls.edu/cyber/cases/concent1.html> (stipulated judgement and permanent injunction).

protect confidentiality, integrity and availability of data and systems. It addresses, for example, denial of service attacks and computer intrusions by making it a crime to "intentionally access a computer without authorization or exceed authorized access." According to experts, the issues involved in technically fraudulent UCE fit uneasily under the statute. Because email is based on trust-based relationships and agreements to move email through the system, proving that an individual has acted without proper authorization may be quite difficult. Other sections of the law might offer relief. For example, where it can be established that a sender of UCE accessed a "protected" computer without authorization with the "intent" to "defraud," and the losses to the entity exceeded $5,000 in a one-year period, a civil action may succeed. [31] The Computer Fraud and Abuse Act provides an existing framework for addressing damage to networks, although it is largely untested in this area. While it may be useful in its current form, changes or additions might provide a sharper tool for addressing the issue of technically fraudulent UCE.

Although some service providers have gained temporary relief from UCE through litigation, such lawsuits are time-consuming and resource-intensive. The outlook from the perspective of end users is even less promising. Few if any end-users have taken senders of UCE to court. Despite some service providers' best efforts to litigate UCE off the Internet, some senders of UCE are quick to target other service providers when faced with a judgment forbidding them from targeting a specific provider. [32] As the president of the Texas Internet Service Providers Association stated, "Anti-UCE litigation is an important tool against UCE. But it seems to have little lasting value against the incorrigible 'guerrilla' spammers." [33] The prevalence of "email harvesting" and "spamming" products continues to produce an expanding pool of new UCE marketers. The company-by-company approach of litigation appears ill-suited to the dynamic environment of UCE.

B. Technical measures [34]

Service providers and technologists are actively devising technical methods of addressing UCE. Most service providers employ a variety of technical methods to identify and defeat UCE and are actively devising and seeking out others. The majority of these efforts fit within the definition of filtering. In addition to filters that are deployed by service providers, mail programs are increasingly adding filters (sometimes called "Bozo Filters") that users can deploy independently.

Filtering options have different implications for service providers and end users. Filtering can take place at the level of the service provider (server) or at the level of the end user (client). At both levels there are two basic kinds of filtering, heuristic and cooperative.

Heuristic filters separate suspect messages based on a set of learned search criteria. Heuristic filters rely on

[31] 18 U.S.C. § 1030(a)(4), (g) (1997).

[32] The myriad of suits filed against Cyber Promotions by various service providers including AOL, Compuserve, Bigfoot Partners and Concentric Network attests to this problem. Recently, Craig Nowak, who was sued by a group of service providers and enjoined by a Texas court from sending further UCE to them, was identified in a case by Hotmail as engaged in sending UCE. Mr. Nowak is negotiating a consent decree in which he will once again promise not to engage in sending UCE.

[33] Gene Crick, President, Electronic Frontiers Texas, President, Texas Internet Service Providers Association, Director, Texas Community Resource Center Internet Access Project, and Editor/Publisher of the Texas Telecommunications Journal, commenting upon the case of Craig Nowak.

[34] For a full exploration of this issue see, P. Hoffman and D. Crocker, Unsolicited Bulk Email: Mechanisms for Control, Internet Mail Consortium Report: UBE-SOL, IMCR-005, October 13, 1997 <http://www.imc.org/ube-sol.html>.

the end-user's or service provider's ability to learn, predict or guess which messages are UCE. They are designed to detect UCE without the cooperation of the message sender. They are either origin-based (filtering based on DNS, IP, etc.) or message-based (filtering based on content). For example, a heuristic filter might eliminate all messages from a certain address or all messages containing the phrase "make money fast." Because origin filtering occurs before a message has been fully received by the recipient's host computer it can reduce many costs associated with UCE. In contrast, message filtering happens after a message is received and therefore service providers don't escape the cost of the initial message processing.

While heuristic filters don't require the cooperation of the sender of email, origin-based heuristic filtering is complicated by falsified header information (DNS, IP, return address). Both origin- and message-based filters are difficult to tailor perfectly — service providers and users must choose between the risk of eliminating some wanted messages or accepting some unwanted messages when choosing a filter. The rules employed in heuristic filters can range dramatically from a simple list of known "spammer domains" to a complex table of rules and variables based on factors such as message origin, routing, relaying and even key words or characters, such as multiple exclamation marks, within the header or message text.

Cooperative filters separate messages with the cooperation of the sender. They can be marked in some fashion, for example, through a label attached by the sender, or they can be identified through some other recognized and standard method, for example, a set of registered domains. A totally effective cooperative filtering system requires a network-wide implementation of, and adherence to, a set of standards for identifying UCE.

Labels allow recipients or their service providers to easily identify and handle UCE as they deem appropriate. Labels can provide a variety of information about the message, such as whether or not it was solicited by the recipient. Similarly, filtering enabled by sender registration allows for easy recipient end message management based on knowledge that the sender is registered as a UCE originator. In contrast, where filtering is based upon recipient registration (similar to an opt-in or opt-out system), the filtering is done by the message sender at the front-end. This shift places the responsibility and burden of controlling UCE upon senders. In either model of cooperative filtering, recipients can continue to receive the UCE they want, if any. They may set their filters or lodge their preferences to block UCE messages, or a subset thereof, or they may specify that they accept UCE. Currently, the incentives for today's senders of UCE to participate in such a system are not always clear — by doing so they may generate consumer goodwill and target only interested recipients, but they will also limit the pool of potential customers and in some models incur direct costs.

In addition to choosing between heuristic and cooperative filtering, service providers and users can choose where to conduct filtering — at the server or the client level. Generally, service providers prefer server-based filtering because it eliminates the costs associated with processing UCE and the need for excess message storage space. Today, many service providers maintain additional server processing capacity and disk space to accommodate UCE messages. By using a server-based filter, a service provider can immediately reject or delete incoming UCE messages, thereby reducing the cost of processing and storing UCE messages.

Client-based filtering is by comparison less effective at eliminating the costs associated with processing and storage by the service provider. Client-based filters place control in the hands of the recipients. Filtering does not take place until messages have been transferred to the end-user or at least her "message store" (temporary storage space on the server).

Client-based filtering can occur in a variety of manners. Users can configure filters, or create separate mail boxes using their mail program, or a service provider may offer subscribers a service whereby they perform this function. Client-based filters require service providers to continue to process and store UCE messages, just as they must with no filtering. While client-based filtering may provide some benefits to service providers (for example, they may lessen the damage to reputation caused by UCE and indirectly limit some hard costs by lessening complaints and storage time) they do not relieve the ISP of many other costs created by UCE.

For end-users, the choice between server-side and client-side filtering is, at least in degrees, a choice between ease and precision. Server-side filtering is often the simpler option for end-users. Server-based filters eliminate UCE without taking the time and energy of the end-user. Client-based filters require users to update personal filters. The economies of scale greatly favor server-based filtering. However, all filtering raises the question, "Who decides what is filtered?" Server-based filtering raises greater risk that the end-user's judgment about what should be filtered is being replaced with the service provider's decision. This may be particularly problematic where filters are set based on factors such as similarity and quantity of messages — which have no direct correlation with the unsolicited commercial nature of a message, but are heuristic devices used to identify probable UCE. Broad heuristic filtering by service providers can prevent users from receiving some messages they want. In addition, server-based heuristic message filtering entails having someone (a machine, not a person) other than the specified message recipient read or scan email messages in order to develop the criteria and weed out unwanted messages. This raises privacy concerns.

The alternative, client-based filtering, can provide end users with a greater degree of control over the content they receive. However, as client-based filters come preconfigured with rules, they too raise questions about who decides what is filtered. They can be personalized and tailored by the user to more precisely meet the individual's needs. When filtering takes place at the client level, the probability of missing desired messages is diminished, and messages need not be read before they reach the end-user. However, because it requires some degree of end-user management, client-side filtering requires users to expend more time and energy dealing with UCE.

As the arms race between service providers and senders of UCE continues to escalate, sophisticated filtering systems are emerging. Unfortunately, some of these systems have proven overly broad. For example, recent news stories report that analysts and free speech advocates are concerned with the preset list of words and punctuation contained in Microsoft's Outlook '98 filter. [35] The filter blocks messages that contain phrases such as "for free!" and blocks messages whose subject lines contain both an exclamation point and a question mark. While the list of terms and punctuation was developed based upon an analysis of more than 2 million pieces of UCE, the filter may block out messages from friends and family. Service providers, like Microsoft, and technologists are continually fine tuning filters to avoid filtering out wanted messages.

The risk of over filtering is higher with heuristic filters. But until most senders of UCE cooperate, heuristic filtering will probably continue to dominate. As a consequence, some wanted mail is likely to be lost, and bad actors will continue to relocate and falsify information, making filtering a less effective tool against UCE.

[35] Lisa M. Bowman, Outlook 98 Filter Goes Too Far, Some Say, ZDNN (Apr. 3, 1998) <http://www.zdnet.com/zdnn/content/zdnn/0402/304002.html>.

IV. CURRENT PROPOSALS

Unsolicited commercial email has captured the attention of companies, individual users, state and federal legislatures, technologists, trade associations, and non-profit organizations. Each has attempted to craft solutions. The result is a wide array of efforts ranging from proposals for new legislation to new technical specifications and new self-regulatory codes of conduct. The proposals reflect various understandings of the problems associated with unsolicited commercial email, as well as the various stake holders' inclinations of how best to implement policy on the Internet. Gauging the potential impact of the various proposals on UCE requires us to consider whether they will remedy the harms suffered by the users, service providers and the Internet itself.

A. Legislative

Current legislative proposals to address UCE take three general forms. Three proposals pending in Congress reflect these varied approaches: [36]

- The Electronic Mailbox Protection Act of 1997 (Senate Bill 875), introduced by Senator Robert Torricelli (D-NJ);
- The Unsolicited Commercial Electronic Mail Choice Act of 1997 (Senate Bill 771), introduced by Senator Frank Murkowski (R-AK); and,
- The 'Netizens Protection Act of 1997 (House Bill 1748), introduced by Representative Chris Smith (R-NJ).

The Electronic Mailbox Protection Act (Torricelli bill) seeks to enable individuals and service providers to reclaim control over incoming unsolicited commercial email by: [37]

- requiring header information to be accurate, which allows individuals and service providers to deploy heuristic filters more successfully;
- prohibiting senders of UCE to interfere with the use of automatic reply functions to respond to messages; and,
- requiring senders of UCE to comply with individual's requests to be removed from future mailings, providing a mandatory "opt-out" for UCE.

[36] A fourth bill, the Data Privacy Act of 1997 (House Bill 2368) introduced by Representative W.L. Tauzin (R-LA) contains a section addressing unsolicited commercial email, and a fifth bill is likely to be introduced by Rep. Merrill Cook (R-CA).

[37] For a copy of the bill and a full explanation of its contents see appendix.

The Unsolicited Commercial Electronic Mail Choice Act (Murkowski bill) incorporates the features of the Electronic Mailbox Protection Act and adds additional sections: [38]

- requiring service providers to filter email for subscribers upon request, and respond to subscribers' and FTC's complaints with respect to UCE; and,
- requiring senders of UCE to tag their messages with the label "Advertisement" in the subject line, which will enable users and service providers to deploy cooperative filtering programs that will block or channel all UCE.

The 'Netizen's Protection Act [39] (Smith bill) prohibits the sending of UCE. Commercial email would only be permitted where an individual has requested it or has a preexisting and ongoing business or personal relationship.

As this report was going to print, the Senate passed "The Unsolicited Commercial Electronic Mail" amendments to the Consumer Anti-Slamming Act of 1998 (Senate Bill 1618). [40] The UCE amendments were sponsored by Senators Murkowski (R-AK) and Torricelli (D-NJ). The UCE amendments require:

- header and routing information to be accurate;
- creators and senders of UCE to provide accurate contact information; and
- senders to comply with remove requests.

The bill provides for both FTC and state government enforcement.

1. Strengths and weaknesses of legislative approaches

The existing legislative proposals provide various degrees of relief from the harms identified by individuals and service providers and have various implications for speech and privacy on the Internet. The relief offered by the various bills range from private rights of action by individuals to statutory fines assessed by the FTC. [41] All three provide users, both individuals and businesses, with greater control over UCE and respond to users' concerns with the intrusiveness of UCE. The Murkowski and Torricelli bills increase users' ability to filter out unwanted UCE and to limit future UCE by requiring senders to abide by requests to cease sending UCE. The Torricelli bill also responds to users' privacy concerns by prohibiting the distribution of email lists for the purpose of UCE where the distributor is aware that any one person does not wish to receive UCE. The Murkowski bill enlists service providers in the battle against UCE by requiring them to offer their users

[38] For a copy of the bill and a full explanation of its contents see appendix.

[39] For a copy of the bill and a full explanation of its contents see appendix.

[40] The Anti-slamming Amendments Act of 1998, H.R. 3888, introduced by Rep. Tauzin (R-LA) takes a similar approach to addressing UCE.

[41] Delving into the appropriate remedial structure for a law addressing UCE is beyond the scope of this report. However, several participants in the working group have noted that private rights of action empower individuals with a tool and, if appropriate statutory relief is structured, an incentive to pursue claims. On the downside, others have noted that the private right of action provided under the TCPA is hindered by the rules of small claims courts and the obstacles to bringing class actions, which would offer a better deterrent. In addition, service providers have voiced some concern with the discovery requests that they could potentially face if thousands of individuals are seeking information from them about the origin of a piece of UCE. Needless to say, in addition to structuring the appropriate rules a statutory approach should carefully structure an enforcement system that provides maximum relief, deterrence and incentives to pursue claims.

filters and to assist the government in identifying and documenting those who violate the law. [42] The Smith bill would prohibit all unsolicited commercial email messages and eliminate intrusions on individual privacy.

Additional protections for privacy that could be incorporated into legislation include limiting the collection of email addresses from public and private spaces, enforcing rules of the forum that limit UCE, limiting the use of email addresses harvested from the Web or chat areas, and prohibiting the use of spamming and trolling programs (similar to the prohibition of automatic number dialing devices by telemarketers).

To a lesser extent, the proposals respond to the cost issues raised by users and service providers. The Smith bill's flat prohibition eliminates the costs associated with unwanted commercial email messages. By facilitating filtering, requiring senders of UCE not to interfere with the ability to use the automatic return function, and to abide by "opt-out" requests, the Torricelli and Murkowski bills each lessen the costs that will be incurred by users. Particularly, the bills will limit the soft costs — time, energy and interference with wanted email — often cited by users. However, Torricelli and Murkowski do allow each sender of UCE to send a message one time — exposing the user and service provider to an initial expense. The labeling requirement of Murkowski's bill will allow for effective filtering which could diminish the cost of even the first message.

The Smith bill would eliminate the hard costs of UCE for both users and service providers. The Torricelli and Murkowski bills will potentially lessen them. As noted above, filtering can greatly reduce the costs, measurable in dollars of resources, access fees, or storage costs, by enabling ISPs to avoid processing and storing unwanted UCE messages.

Creating rules about "proper" UCE messages may increase UCE volume as marketers begin to use a newly legitimized service. However, the opposite effect is possible. Because responding to UCE messages will be easier, enabling individuals to opt-out, UCE volume may decrease.

While each bill would probably lessen the volume of UCE to some degree and facilitate service providers' and users' efforts to control it, which are good for the Internet, their impact on the Internet may vary due to other concerns.

Additional Considerations

2. First Amendment considerations

Legislative proposals to address UCE must be considered in the context of First Amendment free expression guarantees.

a. Banning speech

Banning the use of an entire medium for a specific type of speech — unsolicited commercial email — is a drastic measure. [43] The decision that an entire method of communicating be foreclosed is one that should be made with great caution. Caution is advised not only for the impact it will have on the speech at issue, but also for the model it provides for addressing speech more broadly, especially on the global medium

[42] Several service providers have objected to these sections of the bill because they would burden them with additional administrative and complaint-handling responsibilities.

[43] Working Group members have taken various positions on pending legislation, including H.R. 1748, which would ban UCE. Some have supported H.R. 1748; others have opposed it. Some participants have refrained from taking public positions on legislation at all.

of the Internet. Nations with different ideas and norms about the content that is objectionable may seek to suppress other forms of speech by banning its transmission through email.

The U.S. courts have historically upheld narrowly crafted limits on commercial speech. In considering a ban on unsolicited commercial email, it is useful to examine the courts' approach to bans in other media. In reviewing restraints on unsolicited commercial speech, the courts have been wary of replacing private choice with government bans. However, where privacy considerations are buttressed by measurable cost shifting and an interference with the recipients' ability to receive desired communications courts have upheld bans — for example, the junk fax law. It is unclear whether the cost shifting and interference with desired communications in the junk email context would prove compelling to a court faced with a ban on unsolicited commercial speech.

Where other solutions that avoid regulating speech based on its content have yet to be tested, we should be cautious in adopting a ban. In light of the White Houses' 1997 Framework for Electronic Commerce paper that emphasizes private choice over government imposed content decisions, and given the constitutional issues at stake, proposals to regulate UCE should be pursued cautiously.

b. Labeling

While compelled speech [44] regulations are rarely affirmed by the U.S. Supreme Court, compelled labeling requirements in the commercial context have been upheld. [45] The Court has justified the lesser protection afforded commercial speech on the basis that the government has a substantial interest in guaranteeing that consumers have access to truthful, non-deceptive information regarding commercial transactions. [46] This approach has limited the government to restricting commercial speech in ways that specifically address this interest.

Anxious to preserve the speaker's message, the Supreme Court has said that, "Although the State may at times 'prescribe what shall be orthodox in commercial advertising' by requiring the dissemination of 'purely factual and uncontroversial information,' ... outside that context it may not compel affirmance of a belief with which the speaker disagrees." [47] The section of

[44] Mandatory author self-labeling requirements are compelled speech and raise First Amendment concerns. In general, any regulation that compels speech is content-based and subject to strict scrutiny. Mandatory labeling of all Internet content would also be content-based regulation, because it would compel the speaker to make "statements of fact the speaker would rather avoid." Hurley v. Irish-American Gay Lesbian and Bisexual Group of Boston, Inc., 515 U.S. 557, 573 (1995), citing McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 341-342 (1995) and Riley v. National Federation of Blind of N.C., Inc., 487 U.S. 781, 797-798 (1988). See also, McIntyre, 514 U.S. at 345 ("[E]ven though this provision [prohibiting anonymous campaign literature] applies evenhandedly to advocates of differing viewpoints, it is a direct regulation of the content of speech").

[45] The commercial speech doctrine does not apply to most communication on the Internet. Commercial speech is a highly limited category, applying generally only to advertising and similar speech. See Rubin v. Coors Brewing Co., 514 U.S. 476, 482 (1995) ("[A] test based on '"the commonsense distinction between speech proposing a commercial transaction, which occurs in an area traditionally subject to government regulation, and other varieties of speech"'), quoting Central Hudson v. Public Services Comm'n of New York, 447 U.S. 557, 562 (1980) (citation omitted). Further, expression does not become commercial speech merely because it is sold or involved in a financial transaction. See, Bolger v. Youngs Drug Products Corp., 463 U.S. 60, 66 (1983).

[46] See Consolidated Edison, 497 U.S. at 563.

[47] See Hurley 515 U.S. at 573 (quoting Zauderer v. Office of Disciplinary Counsel of Supreme Court of Ohio, 471 U.S. 626, 651 (1985)).

the Telephone Consumer Protection Act that compels the attaching to all faxes regardless of content the name and phone number of the sender and the time and date sent, [48] has not been considered by the Supreme Court.

Labeling raises fewer concerns than an outright ban on speech. Labels would assist users and service providers in filtering out material. However, from a U.S. perspective, similar to banning, mandatory self-labeling as applied to non-commercial speech, may be unconstitutional. If a solution to the UCE problem rests on mandatory self-labeling, it is important to consider the repercussions for a global medium.

3. Privacy and associational interests

Email may, in a relatively short time-frame, replace traditional postal mail. Due to its increasingly central role in communication, we should carefully think through the consequences of any proposal that would require by law that people either "opt-out" or "opt-in." [49] Both "opt-out" and "opt-in" lists raise privacy and associational concerns — who holds the list, how specific is it, who gets access to it? "Opt-out" proposals may undervalue individual privacy vis-à-vis the interests of commercial speakers. While more protective of individuals' "right to be let alone," "opt-in" lists raise a second privacy concern. Because lists of individuals who wish to receive certain types of information may be far more revealing than lists of those who do not wish to receive information, they may invite greater misuse and abuse.

Recognizing that lists of subscribers already exist in the offline world does not diminish the importance of questioning whether it is advisable to pursue an approach that would generate detailed lists of people's information preferences without establishing appropriate legal safeguards around the information contained in such lists. Recently, the public and policy-makers have registered increased concern with the privacy implications of marketing lists. The consequences of traditional "opt-out" and "opt-in" models, in light of the weak privacy protections afforded the names on such lists, should be thought through before being adopted in this new medium.

B. Technical

Filtering products will continue to enter the market, offering a promising tool to users, both individuals and businesses, and to service providers in their efforts to combat UCE. Filters, critiqued below, are fully discussed in section III. B.

In addition to filters, technologists have developed other tools that address problems associated with UCE. Systems that channel email into various dynamically generated accounts have been proposed and developed. [50] Users limit unwanted email by channeling it to an auxiliary account or bouncing it back to the sender.

[48] 47 U.S.C. § 227(d)(1)(B).

[49] In addition, if email becomes the dominant method of communicating (becoming the 21st century post office and postbox) there may be some other interesting issues. For example, the Court struck down a law that required people who wished to receive "communist literature" to sign-up at the post office — otherwise it would be "filtered" out for them. Lamont v. Postmaster General, 381 U.S. 301 (1965). Requirements that force us to "list" ourselves as interested in particular information may invite some trouble down the line.

[50] Robert J. Hall, How to Avoid Unwanted Email, COMM. OF THE ASS'N FOR COMPUTING (ACM) Vol. 41, No. 3, March 1998, at 88 <http://www.acm.org/pubs/citations/journals/cacm/1998-41-3/p88-hall/>.

A longer version is available from the author at <ftp://ftp.research.att.com/dist/hall/papers/agents/channels-long.ps>.

When dealing with an unknown individual or entity, users can use a distinct email address. If at any time this address becomes a problem due to UCE, or other issues, the user can disable it without hindering her ability to receive other email messages. [51] This technology could potentially provide email users with great flexibility in accepting and rejecting mail from specific senders.

A proposal that has been discussed in Internet technical circles would build upon the channeling concept and create a separate channel for bulk email, the Bulk Mail Transfer Protocol (BMTP). [52] BMTP is intended as an alternative to SMTP, the Internet's Simple Mail Transfer Protocol. By creating a separate channel for bulk email, the protocol would allow end users to register their desire to accept or reject bulk email with their service provider. It would also allow service providers to determine whether to provide bulk mail service to their email subscribers at all. The BMTP also provides for authentication, which would facilitate the implementation of payment schemes where the sender of bulk mail reimburses the recipient or service provider.

Another tool for filtering UCE is referral networks. Acting as a trust mechanism of sorts, referral networks would allow users to reject or separate email messages that have or lack appropriate referral certificates. Users could obtain certificates from other users to whom they wish to send email, or from clearinghouses operated by trusted third parties. [53]

Another set of technical proposals to address UCE would require senders to pay recipients for UCE through either cash or computation. [54] Cash payments accompanying email messages could be made with electronic money. Recipients would have the option of refunding the money to senders of desirable email, but could keep the payment from a sender of UCE. Some have noted that email payment systems would require fundamental changes in the email system, including a large financial infrastructure for what is likely to be relatively low-cost transactions. The system would impose a marginal cost for email transmission on UCE senders, so there would be a disincentive to initiating large bulk disseminations (they would become a lot more expensive), therefore UCE volume would probably decrease. A variant of the cash payment scheme would require payments of computation. Senders of UCE could be required to compute a mathematical function before transferring their messages. Such a requirement would place a significant burden on the computer processing capacity of UCE senders, so fewer messages would be sent. The success of such systems would hinge on wide-spread adoption.

Digital signatures are also being used to address UCE by preventing domain name spoofing. The software,

[51] Lucent's Personalized Web Assistant (LPWA) has provided such a feature to its users since June 1997, for email addresses provided via the Web. Lucent Technologies, The Lucent Personalized Web Assistant (last modified May 7, 1998) <http://lpwa.com:8000/filter.html>. The use of such a feature in general email communications has also been explored. E. Gabber et al., Curbing Junk E-Mail via Secure Classification, PROC. OF SECOND INT'L CONF. ON FINANCIAL CRYPTOGRAPHY, February 1998 (visited June 26, 1998) <http://www.math.tau.ac.il/~matias/papers/fc98-11nc.ps>.

[52] The Internet Mail Consortium provides an organized listing of the various IETF proposals to address UCE. Internet Mail Consortium, IETF Working Groups (visited June 26, 1998) <http://www.imc.org/ietfwgs.html>.

[53] Lorrie Faith Cranor and Brian A. LaMacchia, Spam!, COMM. OF THE ASS'N FOR COMPUTING (ACM) (forthcoming) (visited June 26, 1998) <http://www.research.att.com/~lorrie/pubs/spam/>.

[54] See, P. Hoffman and D. Crocker, Unsolicited Bulk Email: Mechanisms for Control, Internet Mail Consortium Report: UBE-SOL, IMCR-005, October 13, 1997 < http://www.imc.org/ube-sol.html>.

which uses digital signatures to tie domain names to addresses, tackles the problem of UCE with intentionally altered domain names. [55] By providing a mechanism to authenticate domain names, the software will help identify UCE whose true origin has been disguised by the sender. Addressing this common UCE practice will facilitate the detection and filtration of spoofed messages — messages that are often UCE.

1. Strengths and Weaknesses

Filters offer users, both individuals and businesses, tools to control the inflow of UCE and protect privacy by limiting intrusions into the email inbox. Unfortunately, some of the filtering systems have proven overly broad. Using them may put wanted email at risk. The risk of over-filtering is higher with heuristic filters. However, until senders of UCE cooperate, heuristic filtering will continue to dominate. Senders of UCE are unlikely to voluntarily provide information useful for filtering. In fact, many of those who send UCE actively seek ways to hide their identity and disguise the origin of their message to thwart filtering efforts. The prevalence of forged headers makes effective filtering difficult. The development of products that verify domains of origin may assist in filtering efforts.

Server-based filtering (both heuristic and cooperative) helps to eliminate the costs of handling UCE incurred by service providers. While client-based filtering can provide end users with some relief from soft costs (annoyance, infringement on time, interference with wanted email) it does not limit the hard costs of storage and processing incurred by service providers and users. In addition, because client-based filtering requires some degree of end user management, it does not eliminate all the soft costs of UCE.

While limiting service providers' costs, broad heuristic filtering by service providers can prevent users from receiving some messages they want — taking a toll on the free flow of information. In addition, server-based heuristic message filtering entails having someone (a machine, not a person) other than the specified message recipient read or scan email messages. This raises privacy concerns. Filtering is unlikely to affect the overall volume of UCE; therefore it will have little impact on the long term health of the Internet.

Channeling email offers a method for individuals to exercise control over their inbox at the front-end and if they encounter problems at any time down the line. The ability to revoke an email address offers individuals a method of turning off UCE. It can alleviate users' costs of handling UCE. The method used to create the channels may require more computing resources and potentially slow down email. Depending on the number of channels an individual opens, this could be complex to manage and require the user to devote additional time and energy to its upkeep. Referral networks raise similar concerns about computing resources, interference with the sending and receipt of email and resources needed for management.

Overall, technology provides some useful tools for addressing UCE, but currently the tools may require some tailoring and regular upgrades. While various tools can be deployed successfully with or without cooperation from UCE senders (channeling and heuristic filters function in the absence of cooperation), in general, cooperation would increase the utility of technical solutions to combat UCE. The interaction of legislative proposals that require accuracy, domain name verification technology, and heuristic filters holds promise for more consistent and effective filtering.

[55] In October 1997, RSA Data Security gave the Internet Software Consortium (ISC) a free technology license to encrypt and verify domain name system addresses on the fly.

Similarly, labeling requirements found in legislative proposals would greatly ease the task of filtering messages. Without accuracy and/or some cooperation by senders of UCE, users and service providers will have to continue the arms race against UCE and risk the loss of valuable messages.

C. Self-regulatory efforts to address UCE

Many service providers forbid the use of their systems to send UCE. They seek to enforce their terms of service regarding UCE upon both their subscribers and those sending email to their subscribers or across their network. A bill recently introduced in California would allow service providers to bring a civil action against any person violating their terms of service with regard to UCE. [56] To buttress prohibitions on UCE in terms of service agreements, service providers can use technical means to identify and block out-going UCE.

Service providers are potentially able to limit UCE through a number of other self-help or self-regulatory methods. Methods that are currently used to deter UCE include turning off the relay function on routers, which prevents non-account holders from using the service providers system to send UCE. A collaborative effort to limit the ability of UCE senders to co-opt service providers resources is the Real-Time Black Hole (RTBH) initiative. Run by a single individual but subscribed to by several service providers, the RTBH provides a continually updated "black list" of "spammer-friendly" service providers. Service providers seeking to limit the UCE travelling through their system reject all incoming email from those on the black list. Unfortunately, this effort has had some negative repercussions for service providers who, for a variety of reasons, have found themselves on the blacklist. The impact on such service providers and their non-UCE sending subscribers can be serious. [57] To be removed from the black list a service provider must comply with a set of requirements set out by RTBH.

Backbone peering agreements have been identified as another potential avenue for alleviating the cost shifting associated with spam. Peering agreements are the contractual agreements between network providers that establish the terms under which data packets, including email, will move from one network to another. Currently these agreements do not, in general, reflect or compensate the network or service provider based on the level of traffic. However, it is possible to use peering agreements to allocate cost in ways that reflect

[56] Internet Consumer Protection Act of 1998, A.B. 1629, 1997-98 Sess. (Cal.). Introduced by Assemblyman Gary Miller (R-60th Dist.), this bill was supported unanimously by the consumer protection committee of the California Assembly. The committee heard testimony in support of the legislation from representatives of the ISP Consortium, AOL, Netcom, CAUCE, and concerned citizens. The ACLU sent a letter of opposition to the committee. The bill must pass through the judiciary committee and the appropriations committee before it will be voted on by the whole assembly.

[57] One service provider sent the following message to a company whose name had fraudulently been used in UCE and therefore had been erroneously black-holed:

> It has come to our attention that you are providing service to [name deleted], who are operating the web site [name deleted]. This company is offering an opt-out service to prevent Internet abuse, or "spam". While we laud the efforts of your customer we must ask you to disconnect service to him. Opt-out lists are forbidden by our Acceptable Use Policy, due to the fact that they may cause many sites to block [our]...networks. This global problem is effecting all of our customers, and action must be taken. There have been numerous complaints, and more importantly, black-holing (denial of data traffic) of our domain and IP space....Please disconnect this customer within the next 24 hours or we will be forced to take other action.
> Email, 12 June 1998, (author's and recipient's names omitted) (on file with the Center for Democracy and Technology).

network use. In addition to efforts by individual service providers, several associations and organizations have developed self-regulatory proposals to address UCE. Only one of the proposals mentioned in this section of the report is fully operational.

Consumers Connect, Inc. (CCI) offers a free list cleaning service to marketers who send UCE. The service began in June 1997 and is currently used by end-users registered with CCI's opt-out list. Marketers can send their lists to CCI, which will remove the names of individuals who have opted-out and messages that have returned undeliverable replies. CCI does not release the addresses of either end users or of the companies who use the service.

The Direct Marketing Association has proposed a global opt-out database called electronic mail preference system (e-MPS) modeled on their existing mail preference service. Individuals could register their desire not to receive UCE. The service, as proposed, would allow individuals to limit UCE completely, or object to select categories of UCE (for example sports, gardening).

The Association for Internet Marketing (TAIM) is working with software developers to eliminate the stealth features of bulk mailing software which make it possible for UCE to get past filters. TAIM wants to set up an opt-out list for users who do not wish to receive UCE and believes that users should be compensated for receiving UCE. In addition, TAIM believes that service providers should receive a commission for each piece of UCE that is received and examined by an end user.

In contrast to the opt-out approach of e-MPS, CCI, and TAIM, ChooseYourMail provides an opt-in system to address commercial email. Under the ChooseYourMail proposal, users register their email address if they wish to receive commercial email. Email addresses are not made public. If an individual opts-in to receive commercial email, or a subset of commercial email, ChooseYourMail will deliver targeted messages to users on behalf of marketers. Only ChooseYourMail would have access to the list; marketers would pay to distribute their messages to addresses on the list. Service providers would be compensated for accepting messages and would be able to control the timing of message delivery. The ChooseYourMail opt-in program has gained support from ISP trade associations and is currently in test with regional Internet service providers across the country.

1. Strengths and weaknesses

The opt-in approach and to a lesser extent the various opt-out approaches provide individuals and businesses with added control over UCE. While providing individuals with a tool to assert their "right to be let alone," both "opt-out" and "opt-in" approaches raise privacy concerns — who holds the list, how specific is it, who gets access to it? Furthermore, both these approaches work only if senders of UCE are interested in respecting the wishes of the people registering to these lists.

Opt-out and opt-in approaches on their own do not eliminate the costs incurred by service providers, although they may limit costs to users. The payment schemes envisioned by the various proposals would address service providers' concerns with the cost of UCE, however it is unclear whether they would substantially affect the cost to service providers who were intermediaries but not end destinations.

The success of an opt-out approach greatly depends on how widely it is used. In a sense, opt-out and opt-in are similar to cooperative filtering: therein lies the issue. Opt-out and opt-in lists make the sender of UCE responsible for verifying that individuals are willing or unwilling to accept UCE (filter). Both opt-out and opt-in lists are most effective if many or most senders

of UCE cooperate. In today's world, this assumption flies in the face of experience. Today, some senders of UCE employ software to avoid filters, flagrantly violate terms of service statements of service providers limiting UCE, and ignore individuals' requests to be spared future UCE. It is not presently clear what portion of the senders of unwanted UCE would cooperate with voluntary opt-in or opt-out efforts in the future. Until the senders of UCE change their behavior, it is unlikely that opt-in and opt-out systems will provide full relief from UCE. For, unlike the legal and technical proposals, they require senders of UCE to participate actively.

The efforts of individual service providers to limit UCE originating and travelling through their systems have had some impact on UCE. The organizing effort of the RTBH has brought some structure to these efforts and enabled individual service providers to leverage their efforts. Part of their success resides in their ability to take unilateral action. Establishing and enforcing terms of service agreements and black listing those who provide senders of UCE with a gateway to the system do not require the cooperation of those sending UCE. But, like heuristic filtering, such approaches may be overbroad.

To date self-regulatory efforts that require the cooperation of UCE senders has provided limited relief from UCE. However, the Working Group believes that over time, as increased pressure is brought upon senders of UCE, self-regulation may take new forms and may prove more useful.

V. CONCLUSIONS & RECOMMENDATIONS

Providing users and service providers more control over the inflow of UCE is important to the development of email and a short-term imperative. The Ad-Hoc Working Group believes that tools and public policies should advocate end-user control over UCE. Therefore, the Ad-Hoc Working Group recommends that:

- **Technical tools and public policies that allow individuals to indicate their desire to receive or not receive UCE and exercise greater control over incoming email messages should be pursued.**

Filtering offers a useful tool to both users and service providers, acting as agents for end-users, for controlling UCE. However, forged header information and the lack of other definitive methods of distinguishing UCE from other mail make filtering difficult. Therefore, the Ad-Hoc Working Group recommends that:

- **Technical measures and public policies should be pursued that prevent and/or prohibit the use of fraudulent headers to send unsolicited commercial email messages. Such measures will greatly assist users and service providers in managing UCE.**

While filtering enabled by accurate headers, and potentially other information identifying UCE, will help users and service providers minimize some of the costs associated with processing, storing, and reading UCE, the current cost-structure of the email system does not allocate costs in a way that reflects resource usage. A failure to address cost-shifting will leave a central consumer and service provider concern unaddressed. Therefore, the Ad-Hoc Working Group recommends that:

- **Further efforts to examine the cost structure of the email system with respect to UCE should continue to be explored by the private sector.**

Stand alone self-regulatory initiatives generally require the cooperation of all relevant parties. In this case, senders of UCE must participate. Some senders of UCE have shown little interest in the process of self-regulation. Recognizing that the environment is likely to change in ways more conducive to self-regulatory efforts, the Ad-Hoc Working Group believes that:

- **Self-regulatory efforts to create opt-out or opt-in programs should proceed.**

Recognizing that a large portion of UCE is fraudulent — containing deceptive messages — and actively sent in a fashion that thwarts individuals' and service providers attempts to avoid it, the Ad-Hoc Working Group recommends that:

- **Increased efforts to eliminate email fraud be undertaken, and the use of inaccurate and misleading header information be considered an attempt to defraud consumers.**

The Ad-Hoc Working Group urges the Federal Trade Commission, the Department of Justice and relevant state offices to undertake enforcement actions targeting these practices and to clarify their jurisdiction through test cases and other appropriate methods.

The email systems' global nature coupled with its use of standard protocols suggests that the technical community may provide the most effective and scalable tools for addressing the problems associated with UCE. Therefore, the Ad-Hoc Working Group urges:

- **Relevant standard setting bodies to continue to search for technical standards and specifications that will: assist users in controlling incoming email; more fairly allocate the costs of UCE; and ease the burden UCE places on the network.**

The Internet is a dynamic environment. Efforts to solve the problems associated with UCE should be monitored. The Working Group hopes that this report provides a baseline of knowledge and guidance to those seeking to reduce the burdens associated with UCE. Working Group participants look forward to working with others to address this important issue.

AD-HOC WORKING GROUP

The following organizations and companies participated in meetings of the Ad-Hoc Working Group on Unsolicited Commercial Email:

AMERICA ONLINE

1101 Connecticut Ave. NW, Ste. 400, Washington DC 20036
tel 202-530-7878 fax 202-530-7879
www.aol.com

AMERICAN CIVIL LIBERTIES UNION

122 Maryland Ave. NE, Washington DC 20002
tel 202-544-1681 fax 202-546-0738
www.aclu.org

THE ASSOCIATION FOR INTERNET MARKETING

5530 Wisconsin Ave., Ste. 1110, Chevy Chase MD 20815
tel 301-656-1166 fax 301-656-9008
www.taim.org

ASSOCIATION OF NATIONAL ADVERTISERS

700 11th St. NW, Ste. 650,Washington DC 20001
202-626-7800 fax 202-626-6161
www.ana.net

AT&T

295 N. Maple Ave., Basking Ridge NJ 07920
fax 908-221-8484
www.att.com

CATO INSTITUTE

1000 Massachusetts Ave. NW, Washington DC 20001
tel 202-842-0200 fax 202-842-3490
www.cato.org

CENTER FOR DEMOCRACY AND TECHNOLOGY

1634 Eye St. NW, 11th floor, Washington DC 20006
tel 202-637-9800 fax 202-637-0968
www.cdt.org

CHOOSEYOURMAIL.COM

162 N. Franklin, Chicago IL 60606
tel 800-767-6606 fax 312-236-4092
www.chooseyourmail.com

COALITION AGAINST UNSOLICITED COMMERCIAL EMAIL

www.cauce.org
comments@cauce.org

COMMERCIAL INTERNET EXCHANGE

2222 Q Street NW, Ste. 51, Washington DC 20008
tel 202-797-8743
771 Ackley Rd., Cincinnati OH 45255
tel 520-751-8114
www.cix.org

COMPUSERVE

P.O. Box 20212, Columbia OH 43220
tel 614-538-4133 fax 614-326-0560
www.compuserve.com

CONSUMERS CONNECT

P.O. Box 5339, Arlington VA 22205
tel 703-908-9125 fax 703-908-0186
www.ctct.com/ct_main.htm

CYBER PROMOTIONS

DIRECT MARKETING ASSOCIATION

1111 19th St. NW, Ste. 1100, Washington DC 20036
tel 202-861-2407 fax 202-955-0085
www.the-dma.org

EF-FLORIDA

2608 N. Cleveland Cir., Tampa FL 33609
tel 813-871-6052 fax 813-870-0823
www.efflorida.org
scott@efflorida.org

EF-TEXAS

P.O. Box 4570, Austin TX 78765
www.eftexas.org

FLORIDA INTERNET SERVICE PROVIDERS ASSOCIATION

1045 E. Atlantic Ave., Ste. 206, Delray Beach FL 33483
tel 561-266-9438 fax 561-266-9017
www.fispa.org

HOTMAIL

1290 Oakmead Pkwy., Sunnyvale CA 94086
tel 408-222-7030 fax 408-222-7310
www.hotmail.com

IBM

1301 K St. NW, Ste. 1100, Washington, DC 20005
tel 202-515-5062 fax 202-515-5194
www.ibm.com

INTERNET ALLIANCE

8403 Colesville Rd., Ste. 865, Silver Spring MD 20910
tel 301-495-4955 fax 301-495-4959
www.internetalliance.org

INTERNET MAIL CONSORTIUM

127 Segre Pl., Santa Cruz CA 95060
tel 408-426-9827
www.imc.org

INTERNET SERVICE PROVIDERS' CONSORTIUM

100 Washington Ave. South, Ste. 2200,
Minneapolis MN 55401
tel 310-827-8466
www.ispc.org

YOSSI MATIAS

Tel Aviv University, Department of Computer Science,
on leave from Lucent Technologies — Bell Labs

Schriber Bldg. Rm. 305, Tel Aviv 69978, ISRAEL
tel +972-3-6406353 fax +972-3-6409357
matias+cdt@math.tau.ac.il

MCI

1801 Pennsylvania Ave. NW, Washington DC 20006
tel 202-887-3378
www.mci.com/community

MICROSOFT CORPORATION

21 Dupont Cir. NW, Washington DC 20036
tel 202-293-0890
www.microsoft.com

NETCOM ON-LINE COMMUNICATION SERVICES, INC.

2 North 2nd St., San Jose CA 95113
tel 408-881-3227 fax 408-881-3153
www.netcom.com

OMRON ADVANCED SYSTEMS, INC.

3945 Freedom Cir., Ste. 700, Santa Clara CA 95054
tel 408-727-6644 fax 408-272-5540
www.omron.com/oas/index.htm

PEOPLE FOR THE AMERICAN WAY

200 M St. NW, Ste. 400, Washington DC 20036
tel 202-467-4999 fax 202-293-2672
www.pfaw.org

VOTERS TELECOMMUNICATIONS WATCH

www.vtw.org
vtw@vtw.org

WASHINGTON ASSOCIATION OF INTERNET SERVICE PROVIDERS

9445 37th Ave. SW, Seattle WA 98126
tel 206-933-0164 fax 206-935-1923
www.waisp.org

The following individuals and offices attended meetings as observers and/or provided background briefing information. They did not participate in the drafting of this report, nor does it necessarily reflect their views in any way.

FEDERAL TRADE COMMISSION

6th St. & Pennsylvania Ave. NW, Washington DC 20580
tel 202-326-2222 fax 202-326-2496
www.ftc.gov

MARY J. CULNAN

Associate Professor

Georgetown University, School of Business,
Washington DC 20057-1008
tel 202-687-3802

DEPARTMENT OF JUSTICE

1100 Vermont Ave. NW, Washington DC 20530
tel 202-514-2007 fax 202-514-4371
www.usdoj.gov

LYNN MCNULTY

RSA Data Security, Inc.

1420 Spring Hill Road, Ste. 600, McLean VA 22102
tel 703-917-6632 fax 703-448-8208

JOHN MORRIS

Jenner & Block

601 13th St. NW, Washington DC 20005
tel 202-639-6000 fax 202-639-6066

OFFICE OF
SENATOR FRANK MURKOWSKI (R-AK)

322 Hart Senate Office Building, Washington DC 20510
tel 202-224-6665 fax 202-224-5301
www.senate.gov/~murkowski

RON PLESSER

Piper & Marbury

1200 19th St. NW, Washington DC 20036
tel 202-861-3900 fax 202-223-2085

OFFICE OF
REPRESENTATIVE CHRIS SMITH (R-NJ)

2370 Rayburn House Office Building,
Washington DC 20510
tel 202-225-3765
www.house.gov/chrissmith

OFFICE OF
SENATOR ROBERT TORRICELLI (D-NJ)

113 Dirksen Senate Office Building,
Washington DC 20510
tel 202-224-3224 fax 202-224-8567
www.senate.gov/~torricelli

printed as part of the
Digital Issues
series

CENTER FOR
DEMOCRACY
and
TECHNOLOGY

1634 Eye Street, NW Suite 1100
Washington, DC 20006
tel 202-637-9800
fax 202-637-0968
info@cdt.org www.cdt.org

cdt accepts tax-deductable contributions to defray the cost of printing.