Unsolicited Bulk E-mail: The Bane of the Internet

by

Bruce Lane

English 113
Green River Community College
June 1, 2001

Unsolicited Bulk E-mail: The Bane of the Internet

Abstract

The use of electronic mail has enjoyed widespread growth since the Internet got started. It is currently employed by businesses and individuals all over the world as both a substitute for, and supplement to, postal mail, and it shows every sign of eventually becoming as ubiquitous as the telephone.

With this growth has come a serious problem: that of unsolicited bulk E-mail, also known popularly as ‘spam.’ A review of available papers and data by professionals in the Information Technology and Legal fields suggests that spam, if left unchecked by either industry self-regulation or legislative action, will seriously damage the viability of E-mail as an effective communications tool. Within the scope of this paper, spam is a serious and growing problem that must be quickly and effectively addressed if E-mail is to remain a useful resource.

Unsolicited Bulk E-mail: The Bane of the Internet

Background

The vast network of interconnected computer systems that we speak of today as 'The Internet' was never initially intended to carry commercial traffic. It was built to provide a system that scientists and academic institutions could use to share scientific information.

The idea for the Internet began as a simple research paper (Licklider and Clark 1962). After much research, and funding from the U.S. Defense Department's Advanced Research Projects Agency (DARPA), four distantly-located computer systems were linked together. These machines were located at UCLA, the Stanford Research Institute, the University of California at Santa Barbara (UCSB), and the University of Utah, and were fully networked in the latter part of 1969 (Zakon 2000).

The Internet, known then as ARPANET, continued to expand and develop throughout the 70's and 80's. University professors and students, and scientists and staff at various research facilities, were the primary users. Commercial traffic and advertisements were rarely seen during this time, and were generally frowned on. This changed in the early 1990's.

In 1990, a company called 'The World' (world.std.com) became the first provider of commercial dial-up Internet connections to the general public. In 1993, the National Science Foundation created an organization called InterNIC (Zakon 2000) to provide several services, including the registration of new hosts. InterNIC was a joint effort created by the collaboration of three companies on the project: AT&T, Network Solutions, Inc., and General Atomics. Significant commercial use of the Internet began with the first 'banner ads' on web pages in 1994, and the appearance of Internet-based 'malls' (the electronic equivalent of a storefront) such as Amazon.com in 1995.

Today, the Internet has become a critical tool for business and personal communication in our society. It is, therefore, important that everyone who has a need to use the Internet's resources be able to do so with minimal effort. However, connecting to the Internet is a privilege, not a right. Anyone who accepts this privilege also has a responsibility to use what are ultimately limited resources wisely.

There are definite limits on how much traffic the core infrastructure of the Internet can handle, and on the amount of storage space, processing capacity, and connection bandwidth available at Internet service providers and privately-owned host sites. Abuse of the E-mail system, by sending mass unsolicited ads, can overload small systems, rendering them useless to their owners until the overload condition is cleared by trained specialists. Such abuse can also impede, and even destroy, normal E-mail traffic flow to the point where desirable E-mail is lost.

The following paper first describes a brief history of Internet marketing and spamming. Next, the paper will examine the issue of bulk E-mail as an advertising tool. Finally, the paper will draw preliminary conclusions regarding how the abuse of E-mail by unscrupulous advertisers can harm its viability overall, and how correct usage of the system can benefit all users.

Key Definitions

Because this paper involves elements of computer and networking technology, the following terms will aid the reader's understanding.

ARPANET–The progenitor of the Internet. Created by the Defense Department's Advanced Research Projects Agency in the 1960's.

Banner Ad–A form of advertising that places small color graphics, advertising a product or service, on a third-party web page. Clicking on these banner ads usually redirects the visitor to the advertiser's web site.

E-mail–Popular abbreviation for 'Electronic Mail.' The transfer of information between individual users on one or more hosts using SMTP.

Ethernet–A popular type of network technology widely used to create interconnections between host systems in a LAN. Developed by Xerox in the early 1980's.

Host–Any computer or similar information-processing device that is connected to the Internet.

Internet–The network infrastructure that interconnects hundreds of thousands of computer systems all over the world. Originated in the 1960's as the ARPANET, a Defense Department project. Widespread use of the Internet's resources by the general public began in 1994.

LAN–Local Area Network. A collection of interconnected hosts within a small area, such as a home or office building.

RFC–Request for Comments. Documents produced by various Internet working groups (Hauben 1996), including the Network Working Group. The working groups are a voluntary body made up of computer and networking experts in industry, education, and government agencies. All working groups report to the Internet Engineering Task Force, or IETF (IETF 2000) which serves as the Internet's governing technical body.

SMTP–Simple Mail Transfer Protocol. A set of specifications originally defined in RFC 821 (Postel 1982), and redefined in RFC 2821 (Klensin 2001) that define how E-mail is transferred between hosts.

Spam–Popular nickname for unsolicited bulk E-mail. The mass distribution of E-mail messages from one or more sources to hundreds of individuals and/or businesses for the advertising purposes. Also abbreviated 'UBE' or 'UCE' (Unsolicited Commercial E-mail).

T1 Line–A type of high-bandwidth data communications circuit that can be used to provide a dedicated connection to the Internet. T1's have an approximate bandwidth of 1.5 megabits, and typically cost over $1,000 per month to rent or lease.

Usenet–Also known collectively as 'Newsgroups.' A large collection of discussion areas, propagated all over the world. The best analogy for Usenet is that of a categorized public bulletin board where anyone who wants to may post or read a message in any category (Moraes 1998). As of April of 2001, there were over 27,800 newsgroups covering almost every imaginable topic.

Web Site–Nickname indicating the presence of a World Wide Web server, such as www.yahoo.com. These servers provide anywhere from one to thousands of 'web pages,' which are nothing more than text documents carrying special encoding to give them a specific appearance when viewed with a web browser, such as Netscape or Opera.

History and Growth of Internet Marketing: Introduction

The first commercial advertisements on the Internet appeared in 1994 as banner ads on web pages. These ads became widespread as the marketing potential of the Internet became apparent to business users. Within the space of a year, it was nearly impossible to visit a commercial web site that did not feature advertising banners for at least one third party.

The DMA (Direct Marketing Association), an industry trade group founded in 1917 (DMA 2001), was quick to recognize the potential of the Internet in general, and E-mail in particular, as an advertising venue, and has frequently championed both as a marketing tool.

Direct Marketing Growth (Including E-mail)

Table 1, below, sets a baseline for measuring the growth of online marketing. The DMA does not, at this time, have an explicit category for E-mail and banner advertisements. These forms of advertising are considered "Interactive," and are combined in the "Other" category.

Table 1: Direct Marketing Expenditures vs. Total Advertising Expenditures in Billions of Dollars in the United States for 1995.

Medium	**DM Expenditure**	**Total Advertising Expenditure**	**DM Percentage of Total**
Direct Mail	$32.9	$32.9	100%
Telemarketing	50.2	80.9	62.0
Newspaper	13.1	36.3	36.0
Magazine	6.7	12.4	54.2
Television	14.0	37.8	37.0
Radio	4.4	11.3	39.0
Other	10.5	21.9	47.9
Totals	**131.8**	**233.6**	**56.4**

Source: The Direct Marketing Association, 1995, "U.S. Direct Marketing Today Executive

Summary." http://www.the_dma.org/library/publications/charts/dmexp_vs_advexp.shtml
Table 2, below, shows the same data as gathered for the year 2000.

Table 2: Direct Marketing Expenditures vs. Total Advertising Expenditures in Billions of Dollars in the United States for 2000.

Medium	**DM Expenditure**	**Total Advertising Expenditure**	**DM Percentage of Total**
Direct Mail	$44.6	$44.6	100%
Telemarketing	73.2	121.3	60.4
Newspaper	18.4	49.4	37.3
Magazine	9.8	17.3	56.6
Television	21.9	55.3	39.6
Radio	7.7	19.4	39.9
Other	16.0	32.0	50.1
Totals	**191.6**	**339.3**	**56.5**

Source: The Direct Marketing Association, 2000, "U.S. Direct Marketing Today Executive Summary." http://www.the_dma.org/library/publications/charts/dmexp_vs_advexp.shtml

Based on the figures shown, it can be seen that spending for online advertising has jumped from $10.5 billion in 1995 to $16 billion in 2000, an increase of 62.5 percent. Further spending in this category is forecast to grow to $27.7 billion by 2005 (DMA 2001). This represents a potential increase of 277 percent over the 1995 level, almost triple the original figure.
Online marketing is obviously here to stay. The question of which method of online marketing works the best is still hotly debated, especially in regard to E-mail.

Why Spamming is Bad: It Hurts Everyone!

Everyone who had even thought of running a business, or turning an easy profit – con artists and thieves included – were quick to see the potential of the Internet in general, and E-mail in particular. Many had never even heard of the Internet's resources before the 1990's, or simply did not care about how the existing user and administrator base would react to unsolicited ads. These were the people who, ignorant of the network's rich history, saw it and its users as nothing more than a vast untapped advertising venue.

Spamming became popular because it is one of the lowest-cost advertising methods in existence today. A typical dial-up connection can be obtained for between $10 and $30 per month, and the nature of E-mail, at least, is such that it can be easily accessed even with 'legacy' computing hardware as old as 80286-based systems. In fact, anyone can get a start on Internet access with a computer system costing $300 or less, the monthly cost mentioned above, and a standard telephone line.

Once on the Internet, it is a simple matter to begin 'harvesting' E-mail addresses from Usenet news postings, the 'mailto:' links on web pages, and Internet chat rooms. There even exist freely-available software packages, designed to gather such addresses, and create and launch the spamming run, that automate the entire process to the point of "set-and-forget."

Considering that even a modest postal bulk mail campaign of, say, 10,000 pieces can cost $2,300 in postage alone (assuming a bulk presort rate of $0.23 per piece), it is obvious why spamming may look attractive at first glance. However, while spamming may impose minimal costs on the sender, it imposes much greater costs on its recipients in terms of communications bandwidth, server disk space, possible displacement of desirable E-mail, and the increased administration required to deal with mail that was likely unwanted to begin with.

Stolen Resources: A Growing Problem

Consider that, in order to make a return on their investment of a computer and Internet access, a spammer must get as many pieces of their advertising out onto the Internet as possible to insure the highest possible response rate. They know that losing their account is only a matter of time once they start spamming. So, instead of sending their traffic through their provider's mail server, they use their Internet connection to access what is known as an "Open Relay."

An open relay is nothing more than an SMTP server that will accept mail traffic from anyone, no matter what identification they present, and that will then send that traffic on to any recipient, or list of recipients, that the sender presents.

In the early days of the Internet, open relays were not a problem. They were created to provide a measure of redundancy in case one or more mail servers at a given host site were down. The site could, if need be, simply connect to another server at a different site to get their traffic out.

Today, though, operating an open relay is universally frowned upon. Anyone who does so is likely to find their server(s) listed on one or both of two privately-maintained databases of known spam source: ORBS (http://www.orbs.org) or the MAPS RSS (http://www.mail-abuse.org/rss). The result of such a listing is that host sites which subscribe to either or both services can refuse to accept traffic from any host that is running as an open relay.

It is interesting to note that strong philosophical and operational differences exist between the owner/administrators of the ORBS and MAPS sites. As one example of these differences, one will find that the mail servers of MAPS are listed in the ORBS database despite the fact that they are not open relays.

The reasoning behind this, on the part of ORBS, is that MAPS has chosen not to allow the ORBS administrators to actively probe their mail servers, a process that involves sending a brief test message through the target system. If said system is operating as an open relay, the test will be received at a known location.

ORBS performs this type of active probing on an ongoing basis, while MAPS only does so if presented with hard evidence that the server in question has been used to relay spam. The ORBS administrators have chosen to list any system that refuses their probes, even if they know that the system does not run as an open relay. This is one reason why use of ORBS may cause host sites to reject legitimate E-mail traffic. This author has experienced this problem, and has ceased to use ORBS as a result.

Despite the available countermeasures, open relays continue to exist. There are some host sites who have employees and staff that need to connect to their organization's mail server from remote locations.

Other sites are running outdated software that cannot be configured to deny third-party relaying, and the administrators of such sites have chosen, for whatever reason, not to upgrade. There are still other sites who simply do not care that they are wide open as a channel for spammer abuse. The usual reason is that their perception of a "Free and Open Internet" is more important to them than being a good 'network neighbor.'

Open relays are a spammer's best friend, but the use of such to send spam is nothing more than theft by conversion. As one example, some recent spam received by this author was relayed through an open mail server belonging to a school district in Berkeley, California. Leaving aside the issue of theft of computing resources, the possibility remains that the spam run could have overloaded and crashed the school district's mail server, thus depriving the district of needed services. Spammers, however, could not care less as long as they get their traffic out.

In the end, spamming needlessly increases the load on mail servers worldwide. This means increased cost to Internet service providers, in terms of the need to add more powerful systems and additional storage space to handle the load, and in terms of adding additional staff to handle network abuse issues. These increased expenses are then passed on to consumers in the form of higher monthly access fees. Spam even hurts its own senders because they will end up paying higher access costs along with everyone else.

Performing any sort of spam run in today's Internet environment is tantamount to placing a large target on one's back saying 'SHOOT ME, PLEASE!' in bold letters. It is treated, by all but a few unscrupulous ISP's, as an offense that can cost the spammer at least their connectivity, and sometimes money as well.. Some providers assess fines against spammers found on their networks to help cover the cost of cleanup and handling of the inevitable complaints.

The 'Big Three:' The Beginnings of 'Big Spam'

Spamming did not come into being overnight. In fact, the core culture of the Internet itself would not have permitted such an abusive practice to go on any longer than it took to locate the perpetrator's host, and notify the administrator of the site to shut the abuser down.
However, with the general public and 'Big Business' beginning to take notice of what, until then, had been largely a community of academics and scientists, the climate began to change.

In April of 1994, the California law firm of Canter and Siegel, operated by a husband-and-wife team of the same names, gained considerable notoriety by spamming over 6,000 Usenet newsgroups with an advertisement for their immigration or 'Green Card' services (Schwartz and Garfinkel 22-23). The backlash from Internet users and administrators alike was swift and merciless, and eventually resulted in the termination of the firm's Internet access.

Instead of giving up, however, the pair took this as a challenge. After multiple attempts to obtain connectivity from other service providers, and more disconnections for ongoing network abuse, Laurence Canter wrote and published a book called "How To Make A Fortune On The Information Superhighway" (HarperCollins Publishers, 1994). Their last spam hit Usenet in March of 1995, and was an effort to promote the book.

If Mr. Canter was attempting to spawn further network abuse through publication of this book, he most certainly succeeded. In July of 1995, Jeff Slaton, then a sales executive for USWest, read Canter's book. He then decided to spam science newsgroups with ads for what he claimed were plans to make an atomic bomb (Schwartz and Garfinkel 23-25).

He attempted to add legitimacy to this exercise by claiming that he had obtained the data through an unidentified retired researcher from the Los Alamos National Laboratory in New Mexico. It is not known if this claim was true, but Mr. Slaton also claims to have sold hundreds of copies of this plan for $18.00 each, not including postage.

Slaton's spamming activities continued as he offered his services as a spammer-for-hire. He was the first to use fake E-mail addresses and forged domain names in attempts to disguise the origin of his spamming. He was effectively shut down around the end of 1995 through mass exposure by the anti-spam community of, among other things, his photo, home address, home phone number, social security number, and a direct number to his boss at USWest.

In short, he had no further place to hide. He would have faced widespread public humiliation, possible loss of his job, and probable legal action were he to continue his abusive activities.

Perhaps the most notorious spammer in Internet history is Sanford Wallace, owner of Cyber Promotions, a Philadelphia-based marketing company. Wallace was the first spammer to lease a T1 line that he used to host his own domain, cyberpromo.com, for the express purpose of spamming (Schwartz and Garfinkel 25-29). Like Slaton, Wallace offered his spamming services for hire to any advertiser who did not much care about the method used to 'get the word out.'

Unlike Slaton, Wallace was more selective about his targets. He went after AOL (America OnLine) addresses from the start. When AOL blocked all E-mail coming from CyberPromo.com, in an effort to respond to the massive volume of complaints received from its members, Wallace sued the company for infringing on what he declared was his "Right to Free Speech" under the First Amendment.

The argument failed, and the judge in the case ruled against Wallace (Weiner 1996). Shortly thereafter, his problems snowballed as three large Internet service providers – CompuServe, Prodigy, and Concentric Internet – filed their own lawsuits against Wallace and his company.

Not to be deterred, he continued to spam AOL by leasing multiple T1 lines from various providers, and registering different domain names. The resultant change in domain name of the spam's origination point allowed him to get past AOL's filters, at least temporarily.

The legal wrangling, and Wallace's spamming career, came to an abrupt end in March of 1998 when Wallace came under legal attack from Earthlink for spamming its subscribers. He lost that suit as well, and agreed to pay a $2 million dollar settlement that effectively put Cyber Promotions out of business for good.

Wallace now operates a consulting business that reportedly works with its clients to do effective E-mail and online advertising without using spam. It is ironic that one of his clients is the same Atlanta-based law firm (Hunton and Williams) who represented Earthlink in their successful case against Cyber Promotions.

There are still thousands of spammers who continue to emulate the techniques of Canter & Siegel, Slaton, and Wallace. They have a number of techniques for obtaining E-mail addresses, but the most popular ones are 'harvesting' them from Usenet postings, the 'mailto:' link on web pages, and from Internet chat rooms. Some spammers accumulate thousands, or even millions of addresses, rarely (if ever) with the permission of the addressee, and then record them onto CD-ROMs which they will then sell to any willing bulk E-mailer for as much as they can get.

One reason that you should never, under any conditions, respond to a spammer to ask that you be taken off their list is because they have no financial incentive to do so. Your request might get you off of one spammer's list, but said spammer will be just as likely to turn around and sell your address to other spammers as "confirmed active."

Spammers are aided in their activities by unscrupulous Internet service providers (Spamhaus Project 2001). These providers seem to care only for how many monthly accounts they can bill for, and the spammers' activities serve only to further damage the image of advertising E-mail in the eyes of all its recipients.

One example of this damage may be found in a survey of 1,410 random Internet users (Oxman 2000) conducted by the Spam Recycling Center (http://www.chooseyourmail.com). Seventy-one point six percent of the respondents felt that it was at least "somewhat likely" that a spammer had harvested their E-mail address from the respondent's visit to an E-commerce web site. More than fifty percent felt that their address had been harvested from an Internet chat room or news group hosted on a personal or business web site.

Oxman makes reference to a report by IMT Strategies which claims that eighty percent of its respondents have negative feelings towards spam. A more recent report (IMT Strategies 2001) shows that seventy percent of respondents either never responded to unsolicited E-mail marketing, or did so only once.

Given these results, the following can be assumed.

1. Spam is widely disliked.
2. Many Internet users associate visiting E-commerce web sites with getting spammed.
3. The growth of E-commerce is being slowed due to this negative association.

The Case for Legitimate (Opt-In) E-mail Marketing: Permission is the key

Any type of advertising must obviously create a positive impression if it is to be successful. Spam messages are likely to create anything but such an impression. The payload they usually carry is of dubious value at best, and questionable legality at worst. Weight-loss schemes and drugs, investment and chain-letter scams, anti-aging potions, allegedly "free" vacations... all are typical spam content, their exact nature limited only by the sender's imagination and resources.

Any legitimate company who wants to advertise via E-mail may very well be driven away from the idea because they do not want to risk being stigmatized as a spammer. Enter Seth Godin, a computer scientist, graduate student in marketing, and the founder of Yoyodyne Entertainment. Yoyodyne is said to be the 'first company to take E-mail marketing seriously.'

Mr. Godin coined the phrase 'Permission Marketing,' and has published a book about it (Godin 1999). He sold Yoyodyne to Yahoo, Inc., in 1998 for $30 million in shares and the job of vice-president of direct marketing. The term 'Permission Marketing' has now been copyrighted by Yahoo, and it is proving to be a powerful and effective marketing technique both on and off the Internet.

Godin's ideas are unique, and are best reflected in this excerpt (Gauthronet and Drouard 2001).

> "...With the average American today seeing an average of 3,000 advertisements a day, the market is completely saturated. The public's time and attention has been exhausted... Seth Godin warns advertisers that their mass advertising methods are not working... He appeals to them to turn to permission-based direct marketing, in other words, to communicate with customers and prospects on a voluntary basis, slowly building from interest to trust..."

Spam is a form of the very mass advertising that Godin refers to, and is also known as 'opt-out' marketing. This means that permission to send the recipient advertising messages is assumed to exist unless the recipient asks that it be stopped. This is the way postal junk mail has worked for decades, and it is a method that the direct marketing industry has become very comfortable with.

Two key differences between postal mail and spam is that postal junk mail can be opted out of, permanently if the recipient so desires, and that the sender pays the entire cost of sending the material through the postal system. As has already been discussed earlier, this is not the case with spam. Spamming is, in effect, the same as a telemarketer calling someone collect, or someone receiving postal advertising mail with postage due.

As for opting out of spam, it is virtually impossible to get one's address removed from every possible E-mail list that exists because new ones are constantly being compiled. Spammers, lacking any financial or legal incentive to actually honor remove requests, think nothing of selling and reselling, many times over, any E-mail address they can get their hands on.
A good perspective on this problem can be found in this quote from the European Coalition against Unsolicited Commercial E-mail (http://www.euro.cauce.org/en/optinvsoptout.html).

> "...'Individual' opt_out schemes, where the recipient is expected to answer with a 'remove' request, suffer from problems of scale. If only 1% of the USA's estimated 20 million businesses decided to operate in this way, a typical recipient could be... issuing over 200 of these every day for each email address... one sending entity may well honour a "remove" request, whilst passing the address onwards to another... as a "confirmed live" address..."

Again, **everyone pays for opt-out bulk E-mail, even the spammers themselves.** Part of the problem is that the spammers don't seem to care.

Opt-in is an entirely different situation. Opt-in assumes that permission to send marketing E-mail does **not** exist unless the recipient explicitly asks for it in advance. This seems to be exactly the kind of 'permission marketing that Seth Godin refers to, and it has been used to great effect by a few companies, one of the more notable being http://www.chooseyourmail.com. This is a company that appears to have taken Seth Godin's ideas to heart, as illustrated by this quote from Ian Oxman, the company's president:

> "...Founded in January 1998 and funded by International Business Lists... ChooseYourMail began as an investigation into Internet marketing methods and ethics. ChooseYourMail represents an industry wide effort to improve the Internet in three fundamental ways:
>
> 1. Reduce Spam
> 2. Promote privacy sensitive, ethical, "request" marketing.
> 3. Shift costs from the Netizen and ISP to the advertisers
>
> No single strategy will stop spam. A real solution requires email filter technology, legislation, and adverting industry self regulation..."

The opt-in process itself is simple. First, the Internet user locates the web site of a company selling a product or service that the user has an interest in. This discovery may come as the result of hearing about a given site from a friend or family member, or as a result of output from a web search engine, or any number of other sources. The user then examines the site, decides that they would like to be kept up to date on the company's products or services, and fills out an entry to that effect through, say, an electronic form on the same site.

Next, a confirmation E-mail is sent to the user. This E-mail informs them that a request for further information has been made with the advertiser's site, and asking the user to confirm that they did indeed make such a request.

If the user then responds with a positive confirmation, the doorway is open for ongoing advertising E-mail until the recipient asks the company to stop. If the user does not respond at all to the confirmation request, or makes a negative response, no further contact will occur until, and unless, the user once again fills out the electronic form.

The statistics speak for themselves on the subject of opt-in vs. opt-out. The same IMT Strategies survey mentioned earlier showed much higher response rates for permission-based E-mail advertising than for spam. Specifically, a combined response rate of seventy percent between those who responded 'Sometimes' to 'Often.' This means that approximately the same number of people who usually did not respond to spam did respond, positively, to advertising E-mail that they had given permission to receive.

It seems apparent that most Internet users will consider unsolicited advertising E-mail to be spam, while permission-based E-mail is not. While the exact definition of spam is still under debate, two things are clear: Few Internet users enjoy receiving it, and receiving spam damages the image of E-commerce in general, and legitimate (opt-in) E-mail advertising in particular.

Legislation: Effective or not?

Lawmakers, while often slow to respond to change, have considered the problems of spam more than once. In the period of 1999-2001, sixteen pieces of anti-spam legislation have been introduced and debated at the federal level. None have been enacted as yet. However, 21 states have decided not to wait for Congress to act, and have enacted their own local anti-spam legislation (Sorkin 2001).

The most recent piece of federal legislation attempting to deal with spam is S. 630, introduced by Sen. Conrad Burns in late March of this year (Burns 2001). It has come under attack by two anti-spam organizations: The Coalition Against Unsolicited Commercial E-mail (http://www.cauce.org) and Junkbusters (http://www.junkbusters.com).

The attacks, at this time, appear to be justified. S. 630 legitimizes opt-out spamming, and limits enforcement rights to ISP's and the Federal Trade Commission. There is no provision for private right-of-action by end users, the ones who ultimately bear the cost of spam.

Going into detail on some of these provisions will provide a clearer understanding of why some have called S.630 "Bad Law." Note these quotes from the bill's opening statements.

> "...(a) FINDINGS- The Congress finds the following:
>
> (1) There is a right of free speech on the Internet.
>
> (2) The Internet has increasingly become a critical mode of global communication and now presents unprecedented opportunities for the development and growth of global commerce and an integrated worldwide economy... individuals and entities, using the Internet... should be prevented from engaging in activities that prevent other users and Internet service providers from having a reasonably predictable, efficient, and economical online experience.
>
> (3) Unsolicited commercial electronic mail can be a mechanism through which

businesses advertise and attract customers in the online environment..."

The first finding is only partly accurate. Since the Internet is made up almost entirely of privately-owned systems and network links, 'free speech' exists only up to the point where the owner(s) of a given server choose to let it. Spam, being (for the most part) commercial advertising, is not generally protected under the First Amendment. As an unknown systems administrator once pointed out "Free Speech is not free when it comes postage due."

Internet service providers and system owners are not considered "common carriers" (as telephone companies are). They under no legal obligation, outside of that written in their own Terms of Service contract, to allow any form of E-mail or newsgroup posting, or chat room or web site content, that they may feel is inappropriate. Any given ISP, or server owner, has absolute authority over what traffic does and does not transit through their systems, and they have every right to decide which other hosts they will peer with, and which ones they will not.

The second finding is one of the few parts of the bill that appears well thought out, if slightly vague in how it would define 'predictable, efficient, and economical.' However, since spamming is the antithesis of those three words, used together as they were, it would seem safe to assume that the phrasing refers (indirectly) to controlling spam.

The third finding is one thing that has caused the bill to draw such heavy fire from anti-spamming organizations. Unsolicited commercial E-mail is, by definition, 'opt-out,' and it has already been discussed why opt-out marketing is a bad idea.

Perhaps the most disturbing part of the bill is Section 5. The strong influence of the direct marketing lobby can be seen in its phrasing as clearly as if the DMA had written the section themselves. Note the following:

"...(5) INCLUSION OF IDENTIFIER, OPT-OUT, AND PHYSICAL ADDRESS IN UNSOLICITED COMMERCIAL ELECTRONIC MAIL- It shall be unlawful for any person to initiate the transmission of any unsolicited commercial electronic mail message... unless the message provides, in a manner that is clear and conspicuous to the recipient--

(A) identification that the message is an advertisement or solicitation;
(B) notice of the opportunity... to decline to receive further unsolicited commercial electronic mail messages from the sender; and
(C) a valid physical postal address of the sender..."

What the bill is saying, in essence, is that it is acceptable to spam as long as the sender takes steps to identify their traffic as advertising, offer a means to opt out of future mailings, and provide a traceable return address for the sender. No consideration is given to the ultimate cost in time and money that ISPs and end users are forced to bear because of spam, and it seems that no attention whatsoever was paid to the surveys and data quoted earlier in this paper, data which clearly showed that opt-out E-mail marketing is widely disliked, and is not likely to have a good response rate.

Section 6 places enforcement of the bill's provisions almost exclusively with the Federal Trade

Commission. Given that agency's workload, it is unlikely that any spammer other than the largest 'professional' ones would be prosecuted for any violation of the bill's provisions.

The bill does have at least one saving grace: It does not attempt to interfere with any Internet provider setting their own policies against spamming and other forms of network abuse. Note this quote from Section 5.

"...(b) NO EFFECT ON POLICIES OF PROVIDERS OF INTERNET ACCESS SERVICE- Nothing in this Act shall be construed to have any effect on the lawfulness or unlawfulness... of the adoption, implementation, or enforcement by a provider of Internet access service of a policy of declining to transmit, route, relay, handle, or store certain types of electronic mail messages..."

This means that ISPs can still ban spam and spammers from their networks if they so choose. However, given the bill's implicit legitimization of opt-out E-mail, it is likely that there would be a sharp increase in spam traffic should the bill be signed into law in its current form. This means that ISPs and end users would still be forced to bear costs that they should not have to without explicit and advance consent.

As mentioned earlier, many states have taken the matter into their own hands. The strongest of the state anti-spamming laws was enacted in July of 1999 in Delaware (Sorkin 2001). Note the following:

"...§ 937. Un-requested or Unauthorized Electronic Mail or use of network or software to cause same. A person is guilty of the computer crime of un-requested or unauthorized electronic mail:

(a) when that person, without authorization, intentionally or recklessly distributes any unsolicited bulk commercial electronic mail (commercial E-mail) to any receiving address or account under the control of any authorized user of a computer system.

This section shall not apply to electronic mail that is sent between human beings, or when the individual has requested said information. This section shall not apply to the transmission of electronic mail from an organization to its members or where there is a pre-existing business relationship..."

This, in essence, declares unsolicited commercial E-mail itself to be illegal, a declaration that many anti-spam activists and organizations have tried to convince the federal government to make. There is a provision for a pre-existing business relationship, and for unsolicited queries directly from one human to another, such as what might be sent by one relative or other family member trying to locate another. There is also an exclusion for 'opt-in' traffic where the recipient has already asked, in advance, to receive such.

In short, there does not appear to be anything in the Delaware legislation that would not survive a First Amendment challenge, nor that would prevent legitimate opt-in marketing mail. Perhaps Senator Burns should have taken Delaware's actions as an example when he was developing S.630.

It is unclear at this time what direction this legislation, or other bills like it, will ultimately take. One thing, however, is clear: Legislation at the federal level is inevitable. Any Internet user

would do well to make their views known to their elected representatives regarding this bill, or any others which may subsequently appear.

Conclusions

Spam is a controversial issue at best. Marketers would likely prefer that there be no regulation at all of what they can and cannot do regarding E-mail. Common sense, limitations of the Internet's infrastructure, and the very culture of the Internet itself dictate that there must be some form of regulation, or E-mail as we know it will become useless for any purpose.

Permission marketing (opt-in), already being adopted by some companies, appears to offer the greatest chance for striking a balance between the demands of merchants for ad space, and the rights of consumers to make informed choices without being bombarded by advertising that they never asked for. It places control of the consumer's E-mail box much more into the hands of the consumer, and far less into the hands of eager marketers.

Further, opt-in has the potential to generate a much higher degree of brand and company loyalty since the ultimate recipient of the advertising traffic will have asked to receive it to begin with, and because the advertiser showed confidence in themselves, and their products or services, by letting the consumer make the first contact.

Works Cited

Burns, Conrad R. Senator. Can Spam Act of 2001, S.630. U.S. Congress, March 2001. Online. Government web site. 7-May-2001. Available WWW: http://thomas.loc.gov (Place S.630 in the 'Bill Number' field to locate)

Direct Marketing Association. DM Advertising Expenditures by Medium and Market. Self-published, 2001. Online. Organizational Server. 7-May-2001. Available WWW: http://www.the_dma.org/library/publications/charts/dmexp_med_market.shtml

Direct Marketing Association. What is the DMA? Self-published, 2001. Online. Organizational Server. 7-May-2001. Available WWW: http://www.the_dma.org/aboutdma/whatisthedma.shtml

Gauthronet, Serge, & Drouard, Etienne. Unsolicited Commercial Communications and Data Protection. Commission of the European Communities, January 2001. Online. Commission web site. 7-May-2001. Available WWW: http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/spamstudyen.pdf

Godin, Seth. Permission Marketing: Turning Strangers into Friends, and Friends into Customers. New York: Simon & Schuster, 1999.

Hauben, Michael. Netizens: On the History and Impact of Usenet and the Internet. Self-published, June 1996. Online. Columbia University. 7-May-2001. Available WWW:

http://www.columbia.edu/~rh120/ch106.x07

Internet Engineering Task Force. Overview of the IETF. Self-published, 2000. Online. Organizational Server. 7-May-2001. Available WWW: http://www.ietf.org/overview.html

Klensin, J., ed. Request for Comments 2821 - Simple Mail Transfer Protocol. IETF, 2001. Online. Internet Engineering Task Force site. 7-May-2001. Available WWW: http://www.ietf.org/rfc/rfc2821.txt?number=2821

Licklider, J.C.R., & Clark, W. On-Line Man-Computer Communications. August 1962. Online. Digital Equipment Corp., 7-May-2001. Available FTP: ftp://ftp.digital.com/pub/DEC/SRC/research_reports/SRC_061.pdf

Moraes, Mark, et al. What is Usenet? Part 1 of the Usenet FAQ. Self-published, 1998. Online. Private site. 7-May-2001. Available WWW: http://www.faqs.org/faqs/usenet/what_is/part1/

Oxman, Ian. Spam Recycling Center E-mail Users Survey. Self-published, 2000. Online. Private site. 7-May-2001. Available WWW: http://www.chooseyourmail.com/CONCLUSIONS.HTML

Postel, Jonathan B. Request for Comments 821 - Simple Mail Transfer Protocol. IETF, 1982. Online. Internet Engineering Task Force. 7-May-2001. Available WWW: http://www.ietf.org/rfc/rfc0821.txt?number=821

Schwartz, Alan, & Garfinkel, Simson: Stopping Spam - Stamping out Unwanted E-mail and News Postings. Sebastopol: O'Reilly & Associates, October 1998.

Sorkin, David. Spam Laws, United States, State Laws, Summary. Self-published, 2001. Online. Private site. 7-May-2001. Available WWW: http://www.spamlaws.com/state/summary.html http://www.spamlaws.com/state/de.html

Spamhaus Project, The. The Internet's Top Ten Spam Support ISP's. Self-published, 2001 (Continuously Updated). Online. Private site. 7-May-2001. Available WWW: http://www.spamhaus.org/top10.lasso

Weiner, J. Cyber Promotions, Inc. vs. America Online, Inc. et al. United States Dist. Court, Eastern District of PA., 4-Nov-96. Online. Electronic Privacy Information Center. 7-May-2001. Available WWW: http://www.epic.org/free_speech/cyberp_vs_aol.html

Zakon, Robert. Hobbes' Internet Timeline. Self-published, 2000. Online. Private Site. 7-May-2001. Available WWW:

http://www.zakon.org/robert/internet/timeline/#1960s
http://www.zakon.org/robert/internet/timeline/#1990s