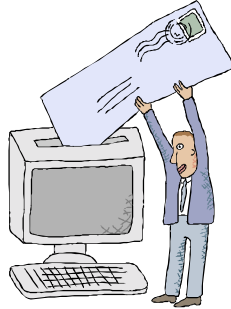


THE SPAM INVASION



University of North Carolina at Chapel Hill
JOMC 223 - Global Impact of New Communication Technologies

December 3, 2003

© 2003 Sandy Bjorkback
bjork@email.unc.edu

UNC Chapel Hill Honor Code

"It shall be the responsibility of every student at The University of North Carolina at Chapel Hill to obey and support the enforcement of the Honor Code, which prohibits lying, cheating, or stealing when these actions involve academic processes or University students or academic personnel acting in an official capacity."

Table of Contents

| | |
|---|--------------|
| Introduction | 1 |
| The Problem with Spam | 1-3 |
| Email erosion, productivity and psychological aspects | |
| Internet fraud (identity theft and scams) | |
| Impact to computer security | |
| Cost implications | |
| Background | 3-6 |
| History | |
| How spam works | |
| The many varieties of spam | |
| National and global legislature | |
| Literature and Resources | 6-7 |
| Filtering | |
| Journalism and sources | |
| Analysis | 7-10 |
| Anti-spammers | |
| Pro-spammers | |
| Viewpoints from the spam debate | |
| Solutions | 10-12 |
| Conclusion | 12-13 |

Introduction

Email is gradually being invaded by its evil offspring, spam. Of course, not to be confused with that perky meat product created by Hormel©, "spam" is the widely used term for Unsolicited Commercial Email (UCE) or Unsolicited Bulk Email (UBE). Spam flows through the caverns of cyberspace until it reaches its intended destination by revealing, disguising or anonymously delivering its virtual face. Initially, the threat of spam was not considered as significant to that of viruses and hacking but now it has become worthy of evaluation on a global scale in both the business and non-business world. The spam invasion is taking over email in ways we may not have imagined in the past. In this essay, I'd like to describe the background of spam, further explore and outline why it is a growing problem and provide perspectives on how to address it.

The Problem with Spam

Why is spam such an issue when a swift flick to the DELETE key can quickly resolve most of the email sorrow it imposes? A key press is only a temporary solution because even when you delete one spam email, there are always more to replace it. Spam is a problematic dimension of email for many reasons. Clearly, spam is invasive and erodes email inboxes and mail servers alike. It's much more than that. Spam reduces productivity and in turn, creates anxiety and tension. From both a consumer and business perspective, it threatens computer security and increases the probability of fraudulent internet spam resulting in identify theft and dangerous schemes. The cost implications of spam worsen as the problem expands. With all of this in mind something must be done to reduce or eliminate the problem spam has created in the online world.

Email erosion, productivity and psychological aspects

Email provides a service at multiple levels for both individuals and organizations. Personal email exchange can be a joyful experience as it keeps open lines with friends, family and acquaintances. Professionally, e-mail's primary usage is for communicating ideas, solutions and making decisions in business. But when a multitude of vigilante spam arrives, it overshadows legitimate email affecting overall communication and productivity. The Harris Interactive study¹ in July 2003 shows that on average, 40 emails per day are received, of which 40% are spam. The time it takes to open email, analyze its validity and take some sort of action can take several seconds to several minutes each. Multiplied, valuable time is lost not to mention the strain accrued on the backbone of the network nervous system hosting the email service. It is estimated that productivity loss could be up to 4 billion in 2003.

From a psychological perspective, spam can invoke emotions ranging from frustration, anger, anxiety to defensive reactions. In some cases, spam can inspire extreme acts of rage within the receiver's environment. Take for instance, the Silicon Valley programmer² who lost control after receiving spam related to "sexual enhancement advertising." His persistent threats to the company who "spammed" him could cost him up to 5 years in prison, not to mention the fines incurred. John Suler, PhD, studies the psychology of cyberspace and also analyzes how spam³ is an invasion of personal space arousing defense mechanisms and anxiety. Some people may immediately delete the email while others are tempted by the persuasive spammer's message.

Internet Fraud (identity theft and scams)

¹ Humphrey Taylor, "Majority in Favor of Making Mass-Spamming Illegal Rises to 79% of Those Online," *Harris Interactive*, http://www.harrisinteractive.com/harris_poll/index.asp?PID=387 (November 25, 2003).

² Reuters, "Male Enlargement Ads Prompt Spam Rage," *CNN.com - Technology*, <http://www.cnn.com/2003/TECH/internet/11/24/spam.rage.reut/index.html> (November 24, 2003).

³ John Suler PhD, "Defending the In-Box: The Psychology of Coping with Spam," *The Psychology of Cyberspace*, <http://www.rider.edu/~suler/psyber/spam.html> (November 18, 2003).

The internet is a great convenience hub for e-commerce but is also being used as a playground to prey on consumers. It's fairly common to provide personal information for online purchases and services. Knowing this, spammers are advantageously using tactics to trick consumers in providing personal information to them (credit cards, SSN, birthdates, etc). Once the spammers have this information, they have an all-access pass to use credit and the consumers' name for their own monetary interests. The FTC provides information on how to minimize the risk of identity theft⁴ relative to spam and recommends not providing personal information via the internet if unfamiliar with the contact. Before sharing personal information, confirm that you are dealing with a legitimate organization. Some recent cases under investigation are those blending identify theft with e-commerce scams claiming to be companies like E-Bay and Pay Pal.

A more dangerous exhibit of spam deception is the Nigerian scam that began circulation in 1995. Spammers claim that they need to transfer money out of the country and promise that if you allow them to temporarily move it into your bank account, 30% of the money will be granted to you fee for service. Fifteen people (14 foreign and 1 American) who actually traveled to Nigeria in this scam were murdered as stated in the US State Department "Nigerian Advance Fee Fraud" document.⁵ It's hard to believe that consumers believed this scam; but they did. We cannot assume people know they are being manipulated. The Secret Service, US Justice and State departments are all involved in this case (referred to as 419) which has yet to be closed.

In 1999, two Russian emigrants in the United States sent more than 50 million emails requesting that consumers send US \$35 to a post office box in Los Angeles. They were targeting colleges and markets where people traditionally are looking for work and money. It was eventually determined that the 2 defrauded victims lost between \$250,000 and \$300,000 (US dollars) and caused over 100,000 complaints to ISPs. They were sentenced to 27 months in prison and fined \$104,000.

Impact to Computer Security

Email is a standard vehicle to receive text, attachments and exchange media between organizations, friends and family. Email is also a perfect way for spammers to distribute viruses, trojans and worms to targeted recipients. The sender's address may be "spoofed" as someone the receiver may know or be listed as unknown with a standard message like "Thank you." Some examples of spam email that has impacted computer security would be the occurrence of the recent mass mailing W32.SoBig⁶ worm that disguised the sender as Pay Pal. It harvested email addresses and attempted to retrieve confidential information such as passwords and credit card information. The key with this one is that it can also setup spam relay servers on the infected system allowing it to spread the worm. Other examples are the W32.Bugbear⁷ worm that hosted a virus which upon opening; shuts down the system's antivirus software, harvests email addresses and can detect keystrokes that pulls credit card / password information. This is a very dangerous and open way to affect a large scale of users.

Cost Implications

As spam continues to flow in, the costs of network hosting services and personnel support will rise as productivity falls. It's logical that an increase in emails would tie up these

⁴ Federal Trade Commission, "ID Theft: When Bad Things Happen to Your Good Name" *Federal Trade Commission For the Consumer*, <http://www.ftc.gov/bcp/online/pubs/credit/idtheft.htm#risk> (November 22, 2003)

⁵ US Department of State, "Nigerian Advance Fee Fraud," *US Department of State Bureau of African Affairs*, <http://www.state.gov/www/regions/africa/naffpub.pdf> (November 22, 2003).

⁶Symantec, "W32.So.Big.B@mm," *Symantec Security Response*, <http://securityresponse.symantec.com/avcenter/venc/data/w32.sobig.b@mm.html> (November 15, 2003).

⁷ Symantec, "W32.BugBear.B@mm," *Symantec Security Response*, <http://securityresponse.symantec.com/avcenter/venc/data/w32.bugbear.b@mm.html> (November 15, 2003).

resources, but what kind of figures are we talking about here? Ferris Research⁸ a collaborative messaging and communication consulting services firm used by major corporations such as Microsoft, Oracle and Sprint, has conducted studies to evaluate the costs of spam. Costs in the US for 2003 are expected to be approximately \$10 billion while 2.3 billion is predicted for Europe. Along with this, there may be a 30% increase⁹ in spam for ISPs. As spam drives up costs, this parallels the need for investment in anti-spam software and increased protection from viruses. Thanks to spam, an industry has risen to fight and establish their own specialized profits!

Along with these problems, the realization is that the global impact of spam continues to worsen over time; especially in North America. From the 2003 UNCTAD's E-Commerce and Development report¹⁰ the rate of spam growth is pummeling the internet. (See Figure 1 below from the UNCTAD report). North America has the highest growth of spam with Asia Pacific and China running closely behind.



Figure 1

Background

The History of spam

The name spam is loosely based on a Monty Python skit where Vikings enter a diner and sing "SPAM SPAM SPAM" to drown out the current conversation.¹¹ That is just how spam behaves; it infiltrates randomly and anonymously to interrupt online flow with invasive emails or pop-up ad messages on a website. It's been stated that the first signs of spam began in 1978 when DEC Corporation sent a mass email to ARPANET¹². Spam has officially been recognized by name since 1994 when the infamous attorney's Lawrence Cantor and Martha Siegel posted a "Green Card Lottery" advertisement to over 6000 news groups on the internet.¹³ The initial intentions of spam for rally of support and profit in an unsolicited

⁸ Ferris Research, "Market Research on Email, Messaging and Collaboration," *Ferris Research*, <http://www.ferris.com/> (November 25, 2003).

⁹ Ferris Research, "Research Focus: Spam," *Ferris Research*, <http://www.ferris.com/offer/spam.html> (November 25, 2003).

¹⁰ UNCTD Secretariat, "United Nations Conference on Trade and Development: E-Commerce and Development Report 2003," *United Nations Conference on Trade and Development*, http://www.unctad.org/en/docs/ecdr2003_en.pdf (November 28, 2003).

¹¹ Joanna Glasner, "A Brief History of SPAM and Spam," *Wired News*, May 26, 2001. <http://www.wired.com/news/business/0,1367,44111,00.html> (Nov 18, 2003).

¹² Brad Templeton, "Origin of the term spam to mean net abuse," *Brad Templeton's Home Page*, <http://www.templetons.com/brad/spamterm.html> (November 7, 2003).

¹³ A.D. Jenson, "Why's it called spam anyway? Spam history and tips," *Epinions.com*, http://www.epinions.com/content_1311023236 (November 10, 2003).

forum continues on today. Spam lives among us but to understand and address it, we need to further evaluate how it works.

How Spam Works

The Center for Democracy and Technology¹⁴ conducted a study in 2002 to find out just how email addresses are obtained by spammers. The findings were that the most prevalent method that spammers use to obtain email address is by searching public websites and newsgroups. This is also confirmed by a spam report conducted in April 2003 by the US Federal Trade Commission (FTC)¹⁵ showing that 86% of the spam harvested email addresses used came from websites and newsgroups. Labor-intensive methods in which spammers get email addresses are by hacking into servers or basically guessing any combination of characters to form an email address. Also, in some cases, email addresses are sold by third parties to spammers. A related news post from CNN online¹⁶ reported that spammers secretly obtained a list of email addresses from the company Orbitz.

Once the spammers successfully compile their list of email addresses, they may be added to a distribution email list or automated script. The spammer decides how to mass populate the email.

The Many Varieties of Spam

Email

Spam morphs into many shapes ranging from health cures, expeditious money-making schemes, investment offerings and sexual / pornographic content. In most cases, spam context is easily identifiable. In SurfControl's "The New Face of Spam,"¹⁷ another type of spam can be "friendly-fire" emails from family and friends consisting of chain letters, jokes and mp3's. This brings spam into a broader category, but what I consider spam is from an unknown sender including unsolicited content.

Based on the official FTC study in April 2003,¹⁸ spam fits into 8 general categories which are listed below. Of these, I have included examples of subject lines pulled directly from emails that have arrived in my very own personal inbox. I did not receive any computer / internet offers which parallels the FTC's finding that only 7% of spam fits into that category.

Type

Investment/Business Opportunity
Adult
Finance
Products and Services
Health
Computer/Internet
Leisure/Travel
Education

Subject

Possibilities to Earn Substantial Income
Does the size of your penis really matter?
Citibank email verification *
The ultimate digital cable filter
Get your order immediately! Viagra
N/A
Just for you: free Caribbean getaway
Earn your Masters in 6 weeks

* Reported to FTC via uce@ftc.gov as this spammer requested my credit card #, pin and SSN. I have yet to receive a response.

¹⁴ Center for Democracy and Technology, "Why Am I Getting All This Spam? Unsolicited Commercial E-mail Research Six Month Report," *United Nations Center for Democracy and Technology*, <http://www.cdt.org/speech/spam/030319spamreport.shtml> (November 18, 2003)

¹⁵ Federal Trade Commission, "False Claims in Spam, A report by the FTC's Division of Marketing Practices April 30, 2003" *Federal Trade Commission: Spam Email - Harvesting Your Email Address*, <http://www.ftc.gov/reports/spam/030429spamreport.pdf> (November 28, 2003).

¹⁶ Reuters, "Spammers steal e-mail addresses from Orbitz," *CNN.com - Technology*, <http://www.cnn.com/2003/TECH/internet/10/30/orbitz.security.ap/index.html> (November 20, 2003).

¹⁷ Paris Trudeau, "Fighting the New Face of Spam: The Rising Tide of Spam Means a Flood of Costs and Risks for Today's Organization," *Surf Control Inc*, http://www.surfcontrol.com/general/assets/whitepapers/New_Face_of_Spam.pdf (November 20, 2003).

¹⁸ Federal Trade Commission, "False Claims in Spam, A report by the FTC's Division of Marketing Practices April 30, 2003" *Federal Trade Commission: Spam Email - Harvesting Your Email Address*, <http://www.ftc.gov/reports/spam/030429spamreport.pdf> (November 28, 2003).

Weblogs and mobile phones

Spam is primarily a problem for email communication but it's not limited to that as it also affects the commenting systems built into weblogs and mobile phone text messaging. Spammers are abusing the comment architecture by posting "blog-spam" advertisements. As a result, some weblog owners have opted not to use comments¹⁹ to minimize spam or have created scripts to blacklist the spammers using tools such as MT Blacklist.²⁰

Mobile phones with text messaging capability are vulnerable to receive spam. There are laws in the US to prevent telemarketers from calling mobile phones (or pagers) such as the FCC's Telephone Communication Protection Act of 1991.²¹ However, there are no laws preventing telemarketers from sending ads to mobile email addresses. This poses problems for consumers who pay for these services. From the Duke Law Journal²², wireless messaging is also a problem in countries such as Japan and Europe. Legislation in the EU is helping reduce the problem in Europe.

National and Global Legislation

United States

Currently, local state governments in the United States have adopted laws to battle the epidemic. For instance, sending unsolicited email in California and Delaware is against the law unless the consumer or business has chosen to receive such emails (opt-in). Pennsylvania and Washington have tailored their anti-spam laws so that it is illegal to send spam with a misleading subject line. Additionally, several states require that advertising spam include "ADV" in the subject line.

For several years, the FTC²³ has been an advocate challenging deceptive spammers by filing lawsuits against them. Of those lawsuits, some cases involved incidents where scammers connected users to their own networks, solicited money for college funding, promised Visas & MasterCard's for a small fee, and offered work-at-home schemes for stuffing envelopes & internet businesses. Victims of these spam scams lost money and time. In an effort to reduce spam at an international level, the FTC has been working with agencies across the world to encourage safe email practices and promote the closure of open-relay email servers.

From the FBI Department of Justice website²⁴, there have been several cases in which spammers have been prosecuted:

- K.C. Smith was convicted to 2.2 years in prison after pleading guilty to two felony charges of securities fraud in 2002. He promised large returns on "international tax-free" investments from a company he made up; "Maryland Investment Club" and spammed his investors until he was finally charged.

¹⁹ Rajeev Sharma, "Death of Email "(Oct 14, 2003),"R-log, <http://unix2.iimb.ernet.in/~rsharma/weblog/000045.html> (November 15, 2003).

²⁰ Jay Allen, "MT-Blacklist," *Jay Allen Dot Org*, <http://www.jayallen.org/projects/mt-blacklist/> (November 28, 2003).

²¹ Federal Communications Commission, "Unwanted Telemarketing Calls," *Federal Communications Commission Consumers and Governmental Affairs Bureau*, <http://www.fcc.gov/cgb/consumerfacts/tcpa.html>, (November 24, 2003).

²² Duke Law and Technology Review, "The Future of Wireless Spam," *Duke L. & Tech. Rev. 0021* (October 28, 2002) <http://www.law.duke.edu/journals/dltr/articles/2002dltr0021.html> (Dec 1, 2003).

²³ Federal Trade Commission, "Law Enforcement Posse Tackles Internet Scammers Deceptive Spammers," *Federal Trade Commission*, <http://www.ftc.gov/opa/2003/05/swnetforce.htm> (November 7, 2003)

²⁴ Department of Justice, "Justice Department Announces Operation Cyber Sweep Targeting Online Economic Fraud," *Department of Justice*, <http://www.fbi.gov/dojpressrel/pressrel03/cyber112003.htm> (November 20, 2003).

- Allan Carlson, a disgruntled "Phillies" fan, was indicted on charges for hacking into computers throughout the US that launched spam criticizing the Philadelphia Phillies baseball team. He was also charged with identity theft because he posed as Philadelphia newspaper reporters in several instances.
- Helen Carr plead guilty for conspiring to possess unauthorized access devices. She used fake email addresses with AOL customers requesting their credit card/personal information to keep their accounts current.

For those spammers who engage in criminal activities such as these, there needs to be some form of regulation and governance. People don't want spam unless they explicitly ask for it. In April 2003, the **CAN SPAM Act**²⁵ (S.877) was introduced to the United States Senate. It was finally passed on November 25, 2003 and is awaiting the Presidents signature. The act trumps any anti-spam state laws in existence. It provisions that unsolicited commercial email be labeled, not include false or deceptive subject lines, include opt-out for user who object to the solicitation and authorizes the FTC to create a "do not email" registry. Penalties include fines, imprisonment based on charges, and possible forfeiture of property / equipment that contributed to the offense.

Of course, it has been said that as more government regulations are imposed and spam increases, this could be the demise of email in violation of the 1st amendment and free speech. I believe this is slight overreaction but definitely something to think about and analyze further.

Other countries (UK, China, Korea, Poland, Italy)

Countries around the globe are fueled up with spam and taking measures against it. According to the BBC News online²⁶ in an effort to ban spam, the UK will fine companies up to £5000 to sending unsolicited commercial mail to individuals without their consent. The drawback of this law is it does not protect business email addresses. The Internet Society of China's Anti-spam Email Coordination team²⁷ blocked 127 servers that were generating spam on 9/9/2003²⁸. In Korea, the Information Minister enacted a law that fines spammers²⁹ for unsolicited email. According to EuroCAUCE,³⁰ Poland and Italy spammers are also punishable by fine.

Literature and resources

Filtering

There is a tremendous amount and variety of online resources available on the topic of spam. However, to narrow the search, the focus for me was in finding information to understand the history and background of spam to then further determine the trends. These trends have helped me outline the problems associated with spam to formulate solutions referenced in this essay in the Analysis, Solution and Conclusion sections. I was able jumpstart this process by filtering from a baseline of keywords including:

- **History/Background:** Spam, about spam, spam history
- **Legislature:** Spam legislature, spam laws

²⁵ Library of Congress, "Bill Summary and Status," *Library of Congress Thomas Legislation on the Internet*, <http://thomas.loc.gov/cgi-bin/bdquery/z?d108:s.00877>: (November 26, 2003).

²⁶ BBC News, "UK Bans Spam Messages," *BBC News World Edition* (September 18, 2003): <http://news.bbc.co.uk/2/hi/technology/3120628.stm> (November 20, 2003).

²⁷ Internet Society of China, "Anti-spam Email Coordination Team of ISC Held 2003 1st Conference," *Internet Society of China*, <http://www.isc.org.cn/20020417/ca134455.htm> (November 20, 2003).

²⁸ Will Sturgeon, "China blocks spam servers," *CNET News.Com* (September 9, 2003): http://news.com.com/2100-1028_3-5073441.html (October 22, 2003).

²⁹ Tim Lemke, "No Slap on the Wrist in South Korea," *The Washington Times* (2003): <http://washingtontimes.com/business/20030901-102352-8411r.htm> (October 14, 2003).

³⁰ EuroCAUCE, "Countries," *EuroCAUCE*, <http://www.euro.cauce.org/en/countries/index.html> (November 20, 2003).

- **Research:** Spam research, spam analysis, spam reports
- **Perspectives:** Anti-spam, Pro-spam, spam weblogs

Relevant journalism and sources

Since spam is a hot technology related topic, online news is a very useful way to get the most current trends and information. I found that CNN Technology and Wired News monitor spam issues quite frequently and have a lot of insightful articles (some of which are referenced throughout this essay).

For legislature, a comprehensive list of links to national, local and international spam laws can be found at the Spamlaws.com³¹ site. The content of this site is managed by David E. Sorkin,³² a spam specialist and associate professor of law at John Marshall Law University. Several government websites reference his site including the United Nations Conference on Trade and Development. For other official sources on legislature and how to deal with spam, I found the Federal Trade Commission, United Nations Conference on Trade and Development and EuroCAUCE a necessary must to discover information.

Many scholars have researched spam but I found a lot of valuable spam-centric information from technology scholar Brad Templeton.³³ He is referenced on several other reputable websites such as the O'Reilly Network.com. He includes essays, theories, solutions and historical information about spam. His perspectives were quite fascinating as he debates the various struggles with spam. Other opinions and resources are from professor of communication Jan Samoriski³⁴ and law student R. Jonas Geissler.³⁵ Both scholars debate how spam legislation may violate the 1st amendment and free speech.

There are not a lot of dedicated spam weblogs available (yet) but I did find The Spam Weblog³⁶ a great source of current spam news links along with a quirky dialog post.

For research information, Ferris Research and Harris Interactive are some of the top consulting companies used to track communication technologies. The United Nations Conference on Trade and Development has been analyzing the growth of the digital economy to help build e-commerce for developing countries. The report³⁷ released in 2003 is a very insightful source to get an overall picture of global spam growth.

Analysis of Spam

Based on the resources and perspectives encountered, spam is no doubt an exponential problem with global affects. Individuals and organizations continuously take measures to protect themselves while spammers formulate slick ways to reach their audience. Most spam originates from the United States with China and Europe being next in line. Wrapped in the heart of the problem are two obvious major players on the spam team: those who support spam (pro-spammers) and those who do not (anti-spammers). The key debates

³¹ David Sorkin, "Spam Laws," *Spam Laws*, <http://www.spamlaws.com/state/summary.html> (November 20, 2003).

³² David E. Sorkin, "David E. Sorkin," *sork.com*, <http://www.sork.com/home.html> (November 21, 2003).

³³ Brad Templeton, "Brad Templeton's Home page," *Brad Templeton's Home Page*, <http://www.templetons.com/> (November 12, 2003).

³⁴ Samoriski, Jan H, "Unsolicited Commercial E-mail, the Internet and the First Amendment: Another Free Speech Showdown in Cyberspace?" Vol. 43, No. 4 (2000), *The Journal of Broadcasting and Electronic Media*, <http://www.umd.umich.edu/casl/hum/comm/spam.html> (November 29, 2003).

³⁵ R. Jonas Geissler, "Whether 'Anti-Spam' Laws Violate The First Amendment," 2001 J. Online L. art. 8, <http://www.wm.edu/law/publications/jol/articles/geissler.shtml> (November 29, 2003).

³⁶ Jason Calacanis "The Spam Weblog," *The Spam Weblog*, <http://spam.weblogsinc.com/> (November 20, 2003).

³⁷ UNCTD Secretariat, "United Nations Conference on Trade and Development: E-Commerce and Development Report 2003," *United Nations Conference on Trade and Development*, http://www.unctad.org/en/docs//ecdr2003_en.pdf (November 28, 2003).

may differ in how to approach the problems associated with spam, especially in regards to legislation and business practices.

Anti-spammers

The majority of users fit into the anti-spammers group and would be more inclined to support the legislation and regulation of spam. Ferris Research found that 79% of users do not support spam at all. What about the remaining 21%? Someone in the cyber galaxy cares about the livelihood of spam. The individuals and businesses receiving spam are ultimately the main victims while pro-spammer and anti-spam software companies are benefiting from it.

Pro-spammers

The internet is appealing for spammers because it is an inexpensive and simple way to advertise and spread messages at a large scale. Breaking down a profile of a spammer is not straightforward because they can be anyone with access to internet resources. There are even support groups such as The Bulk Club³⁸ that promote the spam community and workings of unsolicited emails.

Viewpoints from the spam debate

Since I described in detail the many reasons why spam is a problem, we must analyze the various viewpoints from both sides of the debate that surface in the controversy. Since the majority of users do not support spam, how could anyone possibly defend it? Well, there are a few worthwhile perspectives that crossover from each group that I would like to explore.

What about legitimate email marketing?

In response to a 4 minute blurb on National Public Radio about email marketing, Mitch Wagner posted "*There's no such thing as legitimate spam*" to InternetWeek.³⁹ As for Mitch's statement, unfortunately there are existing "fair and square" email marketing agencies out there such as GOTMARKETING⁴⁰ that use email as a permission-based tool to promote their products. In the US, this form of marketing is supported by the Direct Marketing Agency (DMA)'s working strategy⁴¹ granted the guidelines and any legislation enacted is followed. The SpamCon⁴² foundation is an active supporter of email marketing. These marketing agencies support the CAN SPAM ACT which requires marketers to display their addresses including the opt-out / remove option. As Mitch pointed out, the problem is that the CAN SPAM Act leaves the field wide open for marketers to send email. In other countries such as the EU, the agencies must have consent from the recipient regardless of their business purpose.

I believe the US needs to use more of a European model. Unsolicited email is banned period. Don't give us the option. This is where we need to be. Here in the US, it's starting to become like the John Carpenter⁴³ film "They Live" where black & white subliminal messages are posted all over the city reading "Consume** ** Purchase ** Obey ** Conform" etc. Spam reminds me of that in the persistent way it pushes products and concepts in hopes to persuade or brainwash consumers to participate in their intended cause. I do not believe that marketers have any right sending email (or snail mail) to my personal world without

³⁸ The Bulk Club, "Welcome to the Bulk Club " *The Bulk Club*, <http://www.thebulkclub.com/> (November 28, 2003).

³⁹ Mitch Wagner, "*There's no such thing as legitimate spam*," *InternetWeek.com* (April 17, 2003): <http://www.internetweek.com/newsletter03/04.htm#2003-04-17> (November 28, 2003).

⁴⁰ GOTMARKETING, "Resource Center," GOTMARKETING, <http://www.gotmarketing.com/resources/resources.html> (November 28, 2003)

⁴¹ Direct Marketing Association, "Direct Marketing Agency Anti-spam Working Strategy," Direct Marketing Association, <http://www.the-dma.org/stopsam/workingstrategy.shtml> (November 10, 2003).

⁴² Bobette Kyle, "Direct Email Announcements: Thall Shalt Not Spam," *SpamCon foundation*, <http://www.spamcon.org/marketers/articles/kyle/direct-email.shtml> (November 18, 2003).

⁴³ The Official John Carpenter website, "They Live," *The Official John Carpenter Website*, <http://www.theofficialjohncarpenter.com/pages/themovies/tl/tl.html> (November 29, 2003).

my consent. Anyone that wants to be marketed to should have a right but at least provide the choice.

Also, Wagner brings up the often used marketing defense implying that since several mediums are dominated by ads such as TV commercials, bulk snail mail and so on, then spam should be the same way. His argument is (and I've seen this floating around in other online sources), is the flaw in the marketing defense is the advertiser pays for the delivery costs for these other mediums. This is not true with spam since the costs in most cases are absorbed by the ISP, user or organization hosting the communication services.

What's the big deal? It's just email

"It's just email folks" says Brad Templeton⁴⁴ who states that, "As angry as we get over abuse of E-mail, we must remember that it is just E-mail. The fight to stop abuse is worthwhile, but not worth interfering with important principles of freedom of expression, privacy and individual choice over what can or can't be communicated to them. "

From each of the academic resources, Brad's ideals and spam coverage is premier but I disagree with his statement inferring that spam is not a big deal. Although, our freedoms in any genre are something we should be very cautious in protecting, we cannot use that as an excuse to do nothing against spam. The problems are real. What people transfer to us though virtual or physical means is relevant and should be granted some level of consent on the receiving end. Our freedom should resonate in our rights to decisively choose who invades our territory. It IS a big deal when tons of spam pours in each day violating personal email space, using up network resources, driving up costs and imposing dangerous threats in regards to viruses and the likelihood of fraudulent scam.

Anti-spam legislation: What about the 1st amendment

Communications Professor Jan Samoriski⁴⁵ and law student R. Jonas Geissler⁴⁶ break down how regulating spam could infringe on free speech and the 1st amendment. They do not support anti-spam legislation based upon their belief that this could in part violate free speech and the 1st amendment. Geissler states that "the regulation of email, which is sent and received globally even if the regulation is restricted to computers in the United States, places the United States in the role of policing a world where not all countries share the same values for free speech. The United States has made it official policy to recognize the global quality of the Internet and its limited role in the regulation of the Internet. An attempt to interject itself in the governance and policing of the Internet would be contrary to the established policy of the federal government."

Both Geissler and Samoriski agree that banning *commercial* email violates the 1st amendment and "commercial" email content could be difficult to define. Other regulations such as email labeling may not violate the 1st amendment.

Although I do agree that that defining commercial email may create crevasses for spammer activity, I still don't see how having even a minimal form of regulation could worsen the current situation. Also, even if spammers move their production overseas to escape domestic spam laws we're still better off than we are today. On top of that, legislation in other countries may alleviate some of this activity domestically.

⁴⁴ Brad Templeton, "Statement of Principles," *Brad Templeton's Home Page*, <http://www.templetons.com/brad/spam/prin.html> (November 12, 2003).

⁴⁵ Samoriski, Jan H, "Unsolicited Commercial E-mail, the Internet and the First Amendment: Another Free Speech Showdown in Cyberspace?" Vol. 43, No. 4 (2000), *The Journal of Broadcasting and Electronic Media*, <http://www.umd.umich.edu/casl/hum/comm/spam.html> (November 29, 2003).

⁴⁶ R. Jonas Geissler, "Whether 'Anti-Spam' Laws Violate The First Amendment," 2001 J. Online L. art. 8, <http://www.wm.edu/law/publications/jol/articles/geissler.shtml> (November 29, 2003).

While both Samoriski and Geissler's point are valid, spam vs. the 1st amendment is not as drastic as it sounds. Creating governmental guidelines for unsolicited email does not mean this form of communication would be banned completely. The government has created guidelines for communication such as telemarketing and postal mail so why not email guidelines? I believe that the fact that we don't have a set of consistent email guidelines is an underlying cause of the escalation of the spam problem. The CAN SPAM ACT of 2003 legislation does not violate the 1st amendment based on the actual bill posting at the Library of Congress⁴⁷.

Anti-spam Legislation: Issues with the "Do not email" portion of the CAN SPAM Act

Part of the proposed CAN SPAM Act of 2003 includes a "Do not Email" provision similar to the FTC's recent "Do Not Call" list as a way to opt-out of unsolicited email distribution. Mike Bruner⁴⁸ from MSNC News reported that this could be a problem for marketers and consumers because spammers could get their hands on this list. My thoughts are that they already have their "lists" and if they somehow get access to "Do Not Email" list, then the individual has the responsibility to start reporting or tracking the spammer's address. Although I am in favor of the "Do not email" list, I do see some other issues with it such as the maintenance of changing email addresses and cost of managing this at the government level (will consumers eventually bear the cost anyway?). Also, having such an inclusive list may be a green light invitation for more spammers to send unsolicited emails to those exclusive of it.

Anti-spam legislation: Negative impacts to businesses

Spammers are not the only ones benefiting from their efforts since the anti-spam software industry is becoming a very profitable. Wired, posted an article describing that spammers are not the only ones benefiting.⁴⁹ Spammers could make as much as \$11 million from their schemes while anti-spam companies could gain an estimate of \$653 million. So as we think about legislation and who is fighting for what, spammers are not the only ones affected financially from these decisions.

Solutions to Combat Spam

There are solutions in place today evolving even more as individuals and organizations strategize on battling the spam epidemic. Based on my research, of anything I have experienced on this topic, the "Do Nothing" approach will guarantee repetitive outbreaks of spam. Doing nothing infers pressing the DELETE key and moving on to a second cup of coffee. No, this is not going to help reduce or combat spam. To reduce or hopefully come close to eliminating spam, how do we handle this? I'd like to serve up some solutions to battle the spam problem.

- Support anti-spam legislation
- Filter and block spam at the ISP and mail client/server level
- Block open relays mail servers
- Install and maintain anti-spam/ anti-virus software
- Protect your email address - reduce exposure and diversify
- Graphics – Encapsulate or shelter your email address
- Use common sense

Support anti-spam legislation

⁴⁷ Library of Congress, "Bill Summary and Status," *Library of Congress Thomas Legislation on the Internet*, <http://thomas.loc.gov/cgi-bin/bdquery/z?d108:s.00877>: (November 26, 2003).

⁴⁸ Mike Bruner, "Congress Targeting Outlaw Spam but Firms Still Could Send Unsolicited Ads Under Top Bills," *MSNBC News*: (August 12, 2003) <http://www.msnbc.com/news/948022.asp?0cb=-515171549#BODY> (November 30, 2003).

⁴⁹ Amit Asaravala, "Antispam Companies Raking It In," *Wired News*, (September 9, 2003), <http://www.wired.com/news/business/0,1367,60327,00.html> (November 28, 2003).

Call me old fashioned or conservative (ok, really not) but I do support legislation of unsolicited email. The Senate's recent approval of the CAN SPAM ACT of 2003 ensures that some working solutions may get final approval for unsolicited commercial email including these limitations:

- Label & identify the message as an AD or include a warning if it is sexually oriented
- Cannot include false or deceptive subject lines
- Include a valid return email address
- Include an opt-out feature allowing recipients to be removed from distribution when they object to it.
- Authorize the FTC to create a "do not email" registry.

Although this bill does not cover every possible aspect of spam and may have loopholes for spammers, I am hopeful that these solutions will achieve positive results. I support those limitations but a few additional proposals I have in regards to legislation are that "opt-out", be replaced with "opt-in." With opt-in, only people who WANT to receive unsolicited email would be eligible. This does not include email for companies where consumers chose to be on their email distribution. If the consumer changes their mind and wants to be removed, the companies should honor that. Also, with an "opt-in" inclusion in the CAN SPAM ACT, this would take the burden off the FTC to maintain a "Do Not Email" registry or at least reduce the load.

Filter and block spam at the ISP and mail client/server level

Internet Service Providers should implement filters on mail servers as a service to their customers. While required filters should include immediate rejection of any detected viruses, there should also be spam filtering in place. The difference is that spam filtering should be turned on upon the user's request. These filters can parse out characters, words and patterns based on certain criteria to reduce the amount of spam users receive (for example: SAVE, FREE, \$, MAKE, EARN, etc). ISP's have a responsibility to communicate their policies to consumers and educate them on the tools available.

Additionally, at the email software client level, users may have the ability to block addresses and filter them as well. I know that email programs such as Eudora and Microsoft Outlook have this functionality.

For the more paranoid at heart, email can be setup to only allow in certain addresses. Also, some enhanced email features that require incoming email to be authorized before it is received.

Block open relay mail servers

One of the reasons that it's so simple for spammers to send unsolicited email is due to mail servers throughout the world being configured to accept email from anyone and everyone. Servers with "open" or "insecure" relays allow spammers to disguise their identity to send even higher volumes of email at the expense of the owning organization. These mail servers need to be tightened up to close the relays. Education should be provided for the system administrators of those mail servers. The FTC⁵⁰ is working this from a global standpoint to spread the message to close these open mail relays.

Install and maintain anti-spam and anti-virus software

There is software to fight everything these days and rightfully so. Anti-virus software should be installed on your system or you risk potential damage to your system. For spam there is filtering software available to do the work for you. This takes the weight off your shoulders to configure email for blocking and filtering. But this luxury comes with a price tag.

⁵⁰ Federal Trade Commission, "Open Relays -Close the Door on Spam," *Federal Trade Commission*: (May 2003) <http://www.ftc.gov/bcp/online/pubs/buspubs/openrelay.htm> (November 21, 2003).

Essentially you are allowing software companies to profit in their own way from spam. Regardless, it's a solution.

There's tons of available software on the market. Security software big-boys, Norton and McAfee have both anti-spam and anti-virus software available.

Protect your email address - reduce exposure and diversify

When possible, limit the exposure of your email address in public spaces such as websites or newsgroups because that's how spammers obtain most addresses. Removing your email from websites, chats and newsrooms can help reduce the amount of spam you get. Also, read the fine print when signing up for any type sweepstakes or online services that may request your email address.

Diversify your email address by creating a primary and secondary; maybe one for online purchases and one for fun. This gives higher email availability in case your address is snaked by a spammer.

Graphics – Encapsulate or shelter your email address

Instead of posting your email address as text on websites or weblogs, encapsulate it within a graphic as a .jpg, .bmp or .gif. This way, you can display your email address and reduce the chances that spammers can access you through automation. They can still see your email address but cannot hack through a graphic (at least not yet anyway). This solution will reduce the probability of automated email harvesting. Another way is to remove characters or patterns a spammer may use. Here are some examples of a graphic and a replaced "@" character with the word "at."

bjork@email.unc.edu

or

bjork <at> email.unc.edu

Fight back

If you are constantly getting spammed even after attempts to block and filter, fight back. Based on the situation, try to trace the spammers address and send it to their ISP or report them to the FTC or DMA. A really good resource to help determine how to track down the spammer's email address is based on the email header. The article, "*What Email Headers Tell you About the Origin of Spam*"⁵¹ at http://email.about.com/cs/spamgeneral/a/spam_headers.htm is a really great resource to learn about this.

Use common sense

Upon receiving an email where the recipient is unfamiliar or the content is questionable, do not respond to the sender or merely delete the email. Be skeptical when it comes to providing any type of private or personal information or opening email with attachments to unknown sources.

Conclusion

Spam is a dimension of email that continues to seed itself through the nervous system of the online world. If we continue to let the heartbeat of email live on through spam, we infinitively watch the problem grow and lose valuable time manipulating our networks and inboxes from these cloaked senders. With consideration to the problems brought about by

⁵¹ Heinz Tschabitscher, "What Email Headers Tell You About the Origin of Spam," *What You Need to Know About:* (2003) http://email.about.com/cs/spamgeneral/a/spam_headers.htm (Dec 1, 2003)

spam such as email erosion, impaired productivity and psychological aspects, internet fraud, impact to computer security and cost implications, it's clear that solid working solutions are necessary.

As technology advances to face off with spam, each opponent will unilaterally attempt to conquer each other to fight the invasion, but when will it end? Or will it? Since spam, within itself a growing technology, additional measures are needed to mark any significant improvement to prevent spam from future adaptation. The online world has to let the spammers know "Hey, we've had enough of you."