

SPAM

The Current State

Prepared by: Andrew Leung

TELUS Corporation

Date: August 8, 2003

<i>Definition & Trends</i> _____	3
Introduction _____	3
E-mail Characteristics _____	3
Newsnet Characteristics _____	4
Reasons for Spam proliferation _____	4
Common Spam Tactics _____	6
<i>Impacts of Spam</i> _____	9
<i>Evaluation of Current Anti-Spam Measures</i> _____	11
Common Consumer Counter-measures _____	11
Common ISP Counter-measures _____	12
Common Internet Community’s Counter-measures _____	13
Legislation and Enforcement _____	14
<i>Future Plan of Actions</i> _____	16
Challenges Under the Current Climate _____	16
Proposals for Future Direction _____	18
Issues for further discussion _____	22
<i>Resource References</i> _____	24
Business References _____	24
Technical References _____	26
Government/Legal References _____	27

DISCLAIMER

The views expressed are solely those of the author and do not necessarily reflect the views of TELUS Corporation.

Definition & Trends

Introduction

- Unsolicited, unwanted e-mail messages or news articles sent in bulk to recipients without their permission. In 2002, the Australian National Office for the Information Economy (NOIE) defined spam e-mail as “communication that could not be reasonably assumed to be wanted or expected by a recipient.”
- Spam commonly refers to e-mail because of its popularity (Pegoraro). However, in a more general sense, spam also includes bulk newsgroup articles. As a matter of fact, the word was first used to refer to excessive multiple postings in newsgroup, and then expanded to include junk e-mail.
- Spam is Internet’s version of annoying junk mail, telemarketing calls during dinner, crank phone calls, and leaflets pasted around town, all rolled up into a single annoying electronic bundle.
- Approximately 40% of all e-mail in the Internet is spam, and its volume is growing rapidly.
 - AOL, the No. 1 Internet service provider in US, blocked about 780 million pieces of unwanted e-mail daily, or 100 million more e-mail than it delivered (Washing Post, February 24, 2003).
 - EarthLink, the No. 3 Internet service provider in US, reported a 500-per-cent increase in spam messages to its customers in the last 18 months.
 - Spam is up fivefold over the past 18 months (Vise).

E-mail Characteristics

- Unsolicited Commercial E-mail (UCE) – junk e-mail, e.g. pornographic messages, re-financing mortgage, debt reduction, HGH, Viagra, university diploma, and so on.
- Unsolicited Bulk E-mail (UBE) – lobbying, harassment, personal ranting messages
- Make Money Fast (MMF) – chain letters, get-rich-quick scams, frauds
- Reputation Attacks – venting personal opinion and anger
- The actual volume in size could be higher as spam often contains long messages, and has multi-media attachments.

Newsnet Characteristics

- Excessive Multi-posting (EMP) – identical articles posted to many newsgroups
- Excessive Cross-posting (ECP) - news articles cross-posted to many newsgroups
- Off-topic postings - news articles posted to many inappropriate newsgroups
- Commercial postings – advertising articles posted to many newsgroups

Reasons for Spam proliferation

- Economics of spam - at virtually no cost to spammers, spam reaches millions of potential customers
 - Low e-mail costs translate into cheap direct marketing costs: for CAD \$30/month to pay for ISP connection, anyone can spread ads on a high speed Internet link to reach virtually the whole world.
 - It is easy to do: all one needs to start are a PC with a direct marketing program, and an ISP account for Internet access.
 - People perceive zero real or social costs: “it is just an e-mail.”
 - Spam is the cheapest form of mass advertising and marketing, even cheaper than bulk junk mail:
 - ◆ The costs of bulk mail include paper, printing costs, processing and postage to send their materials.
 - ◆ The marketers can quantify the acceptance percentage of their materials that will be thrown away unread.
 - ◆ Only a small percentage of recipients respond positively to the offerings.
 - ◆ As all three factors remain relatively constant, the amount of bulk mail also remains constant, i.e. it is no more of a problem today than it was a few years ago.

“E-mail-based spam, however, is not yet at economic equilibrium, primarily because the first factor - the cost of sending spam - is more or less non-existent in the e-mail world. It costs spammers almost nothing to send their material.”
(Osterman)

- While costs are negligible, potential payoffs are huge and very profitable:

“Response rates to bulk commercial e-mail are thought to be as low as .005%. That means the typical message appeals to 50 people and annoys 999,950. All the

highbrow defenses of spam start sounding overblown when you consider the sordid reality of the stuff itself--unwanted pyramid schemes, anti-aging gimmicks, and live shower-cam promos. The cacophony drowns out any valuable messages, in any event. It might seem as if the minuscule response rates would doom spammers to failure. Quite the contrary, e-mail is so cheap that they can make money even with almost no click-through. Marketers now pay \$150 for a compact disk with 70 million e-mail addresses--or 3,500 new customers. Not a bad deal. And here's the really troubling development: the economics of spam are only getting worse from a public standpoint. Thanks to aggressive new techniques for harvesting e-mail accounts, the cost of hooking new customers is constantly plummeting." (France)

- People want to make some quick bucks through online marketing.
- Spamming is a legal grey area; it is not illegal in many jurisdictions. Even though spamming may be curtailed or banned by legislation, spammers know that enforcement is difficult, its resources are constrained, and penalties are minor when caught. Other than a few high profile cases involving Microsoft (Festa, <http://zdnet.com.com/2100-1104-985018.html>) and Verizon against Alan Ralsky (Stone; Associated Press), spammers know that they operate in virtual impunity.
- Marketers are not aware of the social or real total costs of their actions. Due to their nonchalant attitude, they will reply any consumer complaints by repeating the same mantra: "If you don't like an e-mail, just delete it."
- Marketers update, re-cycle, and re-use mailing lists for various schemes, and re-sell mailing lists to fellow marketers.
- Marketers have easy access to spamware. The spam phenomenon has spawned a new software market for "spamware," which is commercial software program designed for spamming. Spamware program will harvest addresses, and send mass-mail advertisements in bulk. Capable of running in stealth mode to foil most detection attempts, these programs will forge mail headers, exploit multiple open relays and proxies on the Internet, and randomize message parts to evade mail filters.
- There are commercial spamming services. These service agencies specialize in spamming advertising messages for clients over the Internet.
- Marketers have no difficulties in hopping from one ISP to another ISP due to the intense market competition, even after ISP has cut off their connection services. They also take advantage of free online e-mail services to set up spam accounts.
- There is no universal anti-spamming policy, and enforcement is difficult, especially in the cases of cross-border attacks (e.g. Mexican marketers send spam to Canada)
- "Still wary of anthrax, Americans are opening less junk mail, so marketers are turning to e-mail and phones" (Harrison).

- “The U.S. economy's decline into recession last year had an unexpected impact -- unsolicited e-mail advertisements, known as SPAM, soared” (Schuman).
- It is very difficult to stop spam by ISPs alone: existing technology is not intelligent enough to differentiate legitimate mail from spam. ISPs could also risk litigations on the grounds of invasion of privacy, censorship, and/or impeding freedom of speech and expression.

Common Spam Tactics

- Obtaining e-mail addresses:
 - Marketers run address harvesting programs to scan the entire Internet looking for e-mail addresses that are posted on:
 - ◆ Web sites
 - ◆ Newsgroups
 - ◆ Chat rooms
 - ◆ ICQ
 - ◆ Message boards
 - Marketers buy bulk e-mail addresses online from other marketers: “Spammers can buy direct-marketing lists with, say, a million names for as little as \$19.95” (Black).
 - Marketers run sophisticated programs that guess addresses alphabetically and systematically, (e.g. ann.smith, anna.smith, annabella.smith, annamarie.smith, etc.) and send bogus e-mail to ISPs to harvest valid addresses.

“And here's the really troubling development: the economics of spam are only getting worse from a public standpoint. Thanks to aggressive new techniques for harvesting e-mail accounts, the cost of hooking new customers is constantly plummeting. For example, some programs automatically raid public message boards looking for addresses. Others bombard Internet service providers with random name combinations (asmith@businessweek.com, bsmith@businessweek.com, csmith@businessweek.com) until they hit pay dirt. Such tools are a key reason the volume of spam has exploded in recent months.” (France)

“The method by which spammers harvest email addresses directly from mail servers has been known for years, it's called a 'Dictionary Attack' and both Hotmail.com and MSN.com are highly vulnerable to it due to the sheer volume of email traffic their servers handle each day, traffic in which spammers conducting dictionary attacks can hide undetected literally for many months at a time. Spamhaus has proof that at least one spammer has been conducting a massive dictionary attack against the mail servers of both Hotmail.com and MSN.com, at the rate of 3-4 tries per second, 24

hours a day, continuously for 5 months... Dictionary Attacks work by spammers using software which opens connections to the victim's mail server and automatically submits millions of random addresses, such as "michaelFxy2@hotmail.com", "marla1892@hotmail.com", recording which addresses succeed. These are then added automatically to the spammer's list, which is then resold to spammers world wide.” (http://www.spamhaus.org/action.lasso?-database=sbl_news&-layout=detail&-response=newsstory.lasso&recordID=114&-search)

- Consumers set up auto-reply or out-of-office reply in their e-mail programs, and thus, each reply message is an address confirmation.
- Consumers inadvertently or unknowingly run adware or spyware on their PCs, and allow such programs to harvest addresses, among other private information.
- There are virus or worm programs that attack consumer PCs, and harvest addresses.
- There are hacker attacks that obtain addresses, among other intrusions, from consumers and business.
- Consumers innocently reply to spam to unsubscribe or reject, and each response is an address confirmation.
- Consumers send out E-cards to friends and associates, and both sender and recipient addresses are harvested.
- Business, legitimate or not, sell their own customer addresses for profits, or lose them by accident (McGuire).
- Sending out spam:
 - Marketers send e-mail through known and exploited open relays and proxies on the Internet. Basically, they commandeer Joe Average's PC to route spam through it to cloak their origin and avoid detection. An open relay is simply a mail server, which accepts and forwards messages regardless of their source and destination addresses. Investigators will trace the spam back to Joe, but not to the marketers.
 - Marketers forge sender/return addresses and/or message headers to evade detection or tracking.
 - Marketers schedule their spam programs to activate from mid-night to 6 AM to send out spam to evade detection from ISPs or network administrators.
 - Marketers follow hacker attacks to produce open relays for spam.
 - Marketers throttle the rate of sending e-mail to avoid attracting attention from ISPs or network administrators. They will set the rate low to stay below known threshold, e.g. 10 messages per minute.

- Marketers rotate sender addresses and/or IPs when sending e-mail to frustrate detection attempts.
- Marketers open many spam accounts, especially on free e-mail servers (yahoo.com, hotmail.com, and so on) to vary their sender addresses.
- Marketers hide their identity on the Internet, as id authentication is not required to subscribe to ISPs or e-mail servers.
- Marketers move from jurisdiction to jurisdiction at ease. If Canada bans spam outright, they can move to offshore to resume their spam operations within days.

Impacts of Spam

- The annual cost of spam is estimated at \$8.9 billion for U.S. corporations, \$2.5 billion for European businesses and another \$500 million for U.S. and European service providers according a news story published on January 3, 2003.
(<http://asia.news.yahoo.com/030103/ap/d7oaoc80.html>)
 - Assuming 4.4 seconds for a worker to process a message, spam adds up to \$4 billion in lost productivity for U.S. businesses each year.
 - Companies have to fork over \$3.7 billion to combat spam: more powerful servers, more network bandwidth, and the resulting increased support staff.
 - The rest is the additional help-desk support to users and customers.
- Another cost estimate for spam pegged the total at US\$ 8 billion in 2001.

“A report before the European Commission in February 2001 ([Gauthronet et al.](#)) estimated the cost of spam at 10 billion euro (US\$ 8 billion) per year. This cost is the combination of costs to ISPs and businesses which must handle the traffic and disk storage requirements of spam sent to their users, and the cost in time and in utility to users whose e-mail inboxes are filled with spam” (Krueger).

- ISPs:
 - Install more servers to process and filter spam
 - Add more network bandwidth to process e-mail and spam volumes
 - Suffer denial-of-service attacks under excessive heavy volume of spam, and cease to offer regular services
 - Incur more support costs to install and maintain up-to-date anti-spam measures (e.g. mail filters), field calls from annoyed subscribers, and develop newer protection measures
- Consumers:
 - Spend more time and efforts to go through mailboxes to retrieve legitimate e-mail,
 - Delete legitimate non-spam mail by accident,
 - Update mail filters to screen out spam,
 - Suffer lost email due to false positives, i.e. legitimate non-spam mail is deleted by filter rules,
 - Experience increased user frustration,
 - Perceive spam as a gross act of invasion of privacy, especially due to the offensive nature of many messages, and experience the psychological effect comparable to having home broken into.

- Business users:
 - Spend more time and efforts to go through mailboxes to retrieve legitimate e-mail,
 - Delete legitimate non-spam mail by accident,
 - Feel reluctant to install mail filters for every mail could be a sale order,
 - Have reservations about the effectiveness of e-commerce.

Evaluation of Current Anti-Spam Measures

Common Consumer Counter-measures

- Sift through each message manually to retrieve legitimate e-mail, and delete spam
 - Time consuming
 - Error-prone as legitimate e-mail could be deleted by accident
 - Frustrating
- Install anti-spam and/or anti-virus programs on PC, and configure mail filters (based on subject line, sender addresses, IPs or other criteria) to screen out spam
 - Time consuming to constantly configure and update mail content filters
 - Time consuming to constantly configure and update “white list,” list of addresses from which e-mail will be accepted
 - Time consuming to constantly configure and update “black list,” list of addresses from which e-mail will be rejected
 - Error-prone as false positives could be resulted, i.e. legitimate non-spam mail is deleted by filter rules
 - Frustrating as mail filter rules are set up after the fact, i.e., they work against past spam with known patterns, but may not work against future spam with innovative and subtle contents.
- Set up some accounts on free e-mail service sites as decoys to disguise the actual mailboxes
 - Time consuming to still go through each message manually to retrieve legitimate e-mail, and delete spam
 - Confusing to manage multiple mailboxes
 - Ineffective in the long term, as the actual addresses could still be exposed by friends or associates inadvertently.
- Complain to their ISPs about receiving spam
- Overall, this has become a technological cat and mouse game that consumers by themselves cannot win against the investment and technology mass marketers possess in their disposal. “In addition to the well-known tricks of forging return addresses and mail relays, spammers are adopting new techniques designed to foil filtering software that searches for keywords in messages” (<http://www.internetweek.com/story/showArticle.jhtml?articleID=6900020>). Mail filter is one tool that gives consumers comfort, but by itself, it is not effective against the tidal wave of spam

Common ISP Counter-measures

- Enforce strict no e-mail relay policy for hosts other than its own subscribers
 - Effective against open relay vulnerabilities
 - Time consuming to constantly patch up software to eliminate known exploits
- Establish and publicize AUP (Acceptable Use Policy), and outline procedure handling spamming subscribers; after exceeding threshold of connection attempts, first-time offenders will be given warning, and repeated offenders may lose their accounts
 - Not effective as mass marketers are not deterred at all for they can easily bring their business to another ISP, which welcome them with open arm
 - Not effective as mass marketers can hide or masquerade their identity to foil any authentication attempts
- Install anti-spam and/or anti-virus programs on the server side, and configure mail filters (based on subject line, sender addresses, IPs or other criteria) to screen out spam
 - Time consuming to constantly configure and update mail content filters
 - Time consuming to constantly configure and update “white list,” list of IPs and addresses from which e-mail will be accepted
 - Time consuming to constantly configure and update “black list,” list of IPs and addresses from which e-mail will be rejected
 - Error-prone as false positives could be resulted, i.e. legitimate non-spam mail is deleted by filter rules; AT&T suffered a high profile failure as a result of its spam filter on January 22, 2003 (Olsen, <http://news.com.com/2100-1023-982118.html>)
 - Frustrating as mail filter rules are set up after the fact, i.e., they work against past spam with known patterns, but do not work against future spam with innovative and evasive contents
- Block e-mail from known spam addresses or IPs
 - Time consuming to investigate and verify each spam incident
 - Not effective as the measure works against past spam, but does not work against future spam
 - Not effective as spammers can easily create new addresses or switch to new ISPs or IPs (due to DHCP)
- Block e-mail from blacklisted spam sites or known spam addresses
 - Time consuming to investigate and verify each spam incident
 - Not effective as the measure works against past spam, but does not work against future spam

- Not practical to block large sites, e.g. hotmail.com, aol.com and so on
- Too punitive to penalize an entire site for the infractions of few
- Install authentication measures (e.g. SMTP AUTH) for sending and receiving e-mail; this feature adds security to authenticate senders and/or receivers
 - Effective against non-authorized sending addresses and open relays
 - Error-prone as false positives could be resulted, and legitimate e-mail could be rejected
 - Not practical for business as every mail could be a sale order
 - Not practical for business as every mail could be a sale order
- In his article, Black likens marketers' effort to spread spam throughout the Internet to "Guerilla Warfare" (Black), and another calls it "an e-mail arms race" (Lemos). The spam war pits ISP's technologies against spammers' tricks and innovations. "The more we lock (spammers) down, the more techniques they try to get around us" (Lemos). ISPs alone cannot stop all the spam.

Common Internet Community's Counter-measures

- The Internet community is by nature decentralized since its inception. It tries to perform self-policing and self-regulating functions with mixed results. Most of the efforts are concentrated on maintaining publicly accessible databases of IP addresses of mail servers that relay spam or display abusive patterns. The databases are sometimes known as DNSBL, or DNS-based "Blackhole List." Mail service providers then can query the database(s) when a new e-mail arrives, and block it if it originates from one of the blacklisted sites. Various DNSBLs are maintained; some are commercial offerings chargeable on the number of queries, and some are public services. They offer different policies of adding and removing IPs and ISPs.
- The primary purpose of any blackhole lists is to isolate offending sites. Once isolated by the Internet community at large, a site will be cut off around the world, and its outgoing e-mail will all be rejected. To ISPs, such threats are tantamount to a death sentence. The consequences are so severe that ISPs should be motivated to enforce a tough stance against known and notorious spammers.
- However, the records are checkered.
 - The ORBS facility was shut down due to legal threats on May 31, 2001.
 - ORBS' offshoot ORBZ was shut down on March 20, 2002 under threats of civil and criminal lawsuits. The injunction was from the 10th Judicial District court of the State of Michigan, and ORBZ was alleged to face criminal charges for denial of service.

- MAPS (Mail Abuse Prevention System) was also sued by marketers. Although the lawsuit was settled, MAPS' functions have been curtailed.
- ORDB and SpamCop also face legal intimidations by marketers.
- Some facilities' processes are arbitrary and could be heavy-handed. Mail service providers have very limited time window (e.g. within 24 hours) to resolve a spam complaint against it by even one person. The site addition process is automatic, and the affected site may not be notified at all. Also, the process to remove a site's entry in the database is not just time-consuming, but can also last days. In the meantime, the providers remain black-listed, and their e-mail will be rejected by sites subscribing to the list.
- SPEWS stands for Spam Prevention Early Warning System, and is an extreme DNSBL. It gains its notoriety by operating out of Irkutsk in Russia to avoid marketers' lawsuits that has either shut down or hampered sites, such as ORBS, ORBZ and MAPS. Although it is one of the most effective blackhole lists, SPEWS is also highly controversial because of its anonymous operation and aggressive policy against ISPs.

Legislation and Enforcement

- Industry Canada's stance regarding spam was first articulated in a paper titled "Electronic Commerce in Canada" (<http://e-com.ic.gc.ca/english/strat/spam.html>), which was written in July 1999.
- Another pertinent legislation is The Personal Information Protection and Electronic Documents Act, or Bill C-6, (http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp). The act was accent on April 13, 2000, and has been coming into effect over three stages from January 1, 2001 to January 1, 2004. The Privacy Commissioner of Canada enforces this privacy legislation.
 - The two relevant sections, 4.3 and 4.3.5 only govern mailing lists, not spam per se. The law stipulates that companies collecting e-mail addresses should seek consent from the address owners.

“4.3 Principle 3 - Consent The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate. Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or

inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.”

“4.3.5 In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.”

- “The amount of unsolicited, junk e-mail you receive as a result of your travels around the Web can be an annoyance, but this "spam" is only the most obvious privacy problem” (http://www.privcom.gc.ca/fs-fi/02_05_d_13_e.asp).
- “The Canadian situation regarding legislation dealing with spam is not very good” (<http://cauce.ca/situation.html>).
- “Currently there is no anti-spam legislation in Canada; however, seriously disruptive spam may be prohibited by Canadian criminal law” (Bennet).

“Canadian policy on spam was last articulated in the late 1990s in a policy document from Industry Canada's electronic commerce branch. The government acknowledged the public's rising concern with spam but cited several reasons why it believed new legislation was unnecessary. First, the government argued that consumers could consider the anti-spam measures employed by their Internet service provider when picking their provider. If their ISP wasn't doing enough to counter spam, they could simply shift their business elsewhere. Second, the government claimed that Canada's new privacy legislation would help guard against the buying and selling of personal e-mail lists that are the lifeblood of spammers. Third, it maintained that the courts could be used to battle spam, either through civil lawsuits or by using the Criminal Code to bring criminal charges where the offending spam was fraudulent or otherwise illegal in nature... Although the legislation would indeed apply to the sale of personal e-mail information without consent, this approach targets list brokers, who buy and sell e-mail addresses for pennies per thousand, rather than the spammers themselves” (Geist).

Future Plan of Actions

Challenges Under the Current Climate

- Although spam is commonly referred as “unsolicited commercial e-mail,” the definition itself is vague, and very subjective.
 - Only the recipient is in the best position to determine whether or not an e-mail is actually solicited. Some consumers subscribe to mailing lists that other consumers may associate with spam. However, such subscriptions are based on individual preference, and there is no uniform standard. In addition, even consumers may not clearly know how many subscriptions they own, especially if they subscribe to many.
 - The “commercial” nature or tone of an e-mail is also difficult to determine, especially by software technology. Moreover, mass marketers have become more subtle in their approach, and made it harder and harder to detect.
 - In short, only the recipients can truly differentiate legitimate e-mail from spam. Therefore, the unclear and subjective definition of spam has made it difficult to implement any effective anti-spam measures, especially from ISP’s perspective. To set up an effective mail filter for a customer, an ISP must customize it to an individual’s preferences, including white and black lists. The ISP must track the usage pattern and history on the Internet in order to compile a valid subscription list in which the customer has opted. Even then, the filter may still produce false positives if one of the customer’s long-lost friends sends a greeting message. If the filter merely sidelines suspected e-mail for manual processing later, instead of deleting e-mail, the whole purpose of mail filtering is defeated. Moreover, such filter customization is expensive, and its cost may be prohibitive to consumers. Also, there are legal implications of compiling the individual preference and usage history, and the efforts to build a better filter may be perceived as an infringement of privacy, censorship or even an impediment of the freedom of speech and expression.
- At present, the whole cost and benefit equation of spamming is entirely tilted in favour of mass marketers, and stacked against the rest of the society.
 - Only the spammers benefit from rampant electronic advertising. They make more sales and more profits. For added measures, they can re-sell the list of addresses to other mass marketers for even more returns.

- While it costs marketers next to nothing to spam, the rest of the society bears the entire burden of cost.
 - ◆ ISPs must pay additional hardware, software, network bandwidth, and support to combat spam and install anti-spam measures. Mail filtering technology is not only expensive, but also developmental: "Spam-filtering is shooting at a target that is not just moving, it's taking evasive action" (Kane, <http://news.com.com/2100-1023-981177.html>).
 - ◆ The Internet community spends time to tabulate list of spam sites for blocking purpose, but their efforts have been undermined by marketers' legal maneuvers and litigations.
 - ◆ Consumers must pay for anti-spam software and spend time to constantly update mail filters that are not effective. Ultimately, all these costs born by ISPs and the Internet community inevitably will pass on to the consumers. Also, with the advent of new communication devices, they will pay more when they use services such as wireless e-mail, e-mail paging and so on. These services charge consumers based on usage or air time, and the more spam they have to sift through, the higher the usage. Spam will impact consumer adoption of these and other new communication services.

“E-mail marketing is fast, effective and dirt cheap — a godsend for marketers in an economy that has crunched advertising budgets. Zipping an electronic ad to your mailbox costs a marketer about 5¢, compared with 25¢ to \$3 for the postal equivalent. And e-mail marketing works. The Direct Marketing Association, which represents nearly 5,000 companies that send both postal and electronic direct mail, announced at its conference last month that two-thirds of its member companies reported increased sales from e-mail, which generated an average of 15% of their online sales — up from 3% in 2000. Because it's so easy to click from an e-mail to a website's "purchase" button, an e-mail campaign can reap up to 12 times the response rates of ordinary junk mail.

Little wonder that old-line companies like Ford and Procter & Gamble are joining early users of targeted e-mail pitches like Amazon.com and J. Crew. Corporations will spend \$1.8 billion on e-mail marketing this year and \$6 billion by 2005, according to Forrester Research. It's a ticklish irony that the humble medium of e-mail is blossoming.” (Takeuchi Cullen)

- In summary, society at large bears the costs of the infraction of a few spammers, who reap all the benefits. The cost and benefit equation of spamming is absurd and impertinent.
 - At present, the ISP industry, consumer and consumer groups, the Internet community, and government jurisdictions take up most anti-spam measures independently and separately. So far, there is no concerted effort to coordinate all stakeholders to deliver a comprehensive solution.
 - There is no clear government legislation on curtailing spamming activities in Canada. Hence, mass marketers can operate with impunity, and spamming has flourished in this legal vacuum.

Also, any efforts by ISPs, consumer groups, or the Internet community will be hampered by the threat of lawsuits on the constitutional grounds of violating freedom of speech and expression, invasion of privacy, and/or censorship.

Proposals for Future Direction

- The government should enact new legislations to curtail, restrict or ban spamming activities. Specifically, the new law should alter the cost benefit equation to discourage spam through increasing its costs. For instance, mass marketers will start paying for the economic and social costs of spamming, and thus, will make spamming much less profitable and more punishable. “So, what will it take for the economics of spam to reach equilibrium? The most important factor will be a dramatic increase in the cost of sending spam” (Osterman). By hitting the bottom line and threatening with fines and penalties, mass marketers will think twice about their spamming activities. No anti-spam measures are effective unless legislators intervene, similar to the case of stopping fax spam through legal amendments and remedies. The ultimate goal is to introduce financial and legal incentives in order to influence and encourage marketers, of which many are legitimate business, to act responsibly.

“Quite simply, consumers bear the cost of spam regardless of which ISP they choose. Each provider employs a battery of marginally effective anti-spam measures that require significant resources. The cost of those resources is ultimately borne by the consumer, who indirectly pays not to receive spam... Moreover, some Internet users actually pay to receive spam. New e-mail devices such as Research In Motion's BlackBerry frequently charge users based on the amount of data they download. The more spam a user gets, the more he or she pays... it has become clear that a market-based solution unacceptably leaves consumers paying not to receive spam. The time has come to hit the delete key on current weak Canadian anti-spam policy and to begin work on crafting legislation that better protects Internet users.” (Geist)

“David J. Farber, former chief technologist at the Federal Communications Commission, doubts filters can ever be a complete solution to the spam plague--a verdict increasingly shared by other technology experts. That's why it's time for a legal assault. Already, more than two dozen states have passed measures against garbage mail. California, Colorado, and five other states, for instance, now require mass e-mailers to label advertising missives "ADV:" in the header line, which makes them much easier to block with filters...

This development means one simple thing: that private solutions to curbing spam won't work. This is a classic case of free-market failure. Consumers can ignore junk e-mail to their hearts' content, but no amount of rejection will ever make mass e-mailing

unprofitable. Only the government can change the cost-benefit analysis enough to make a difference.

Of course, these steps would not kill junk e-mail. Offshore e-mailers, including many of the Net's most notorious scam artists and pornography merchants, could still invade U.S. in-boxes at will. Indeed, this loophole is often cited as an argument why spam shouldn't be regulated at all. But the problem is exaggerated. Well over half of all bulk commercial e-mail, including most of the offers for legitimate products and services, originates domestically, according to Brightmail CEO Enrique Salem.

Although it isn't easy to do so, senders can be tracked down and prosecuted--a prospect that, by itself, would frighten many spammers into compliance. Look at the junk fax law, which has all but eliminated that once-widespread problem.” (France)

- The government can require marketers to add the prefix “ADV:” in the subject line of mass mailouts. The label will distinctively mark mass e-mailing, and make mail filtering immensely more effective. Even if the label cannot eliminate spam, it add costs to spammers. For example, if the label is only 80% effective against identifying spam, marketers’ costs increase by 4 times; if the efficacy rate is increased to 90%, the costs will raise by 9 times. In addition, consumers now can make a rational choice with the confidence that the action will reduce spam in their mailboxes.
- The government can strengthen and expand the existing Personal Information Protection and Electronic Documents Act. First, the act should retroactively recognize all e-mail addresses as private properties, instead of since the enactment day. Secondly, the act should enforce the concept of consumer “opt in” in mass e-mailing. For instance, marketers should explicitly receive consent from customers before mailouts, and provide an easy way for customers to opt out later.
- The government could shield ISPs, software makers, consumers and the Internet Community from lawsuits and litigations when they engage in activities protecting consumers from spam. When companies and organizations band together to reduce spam, they should not work under the shadow of litigations that aim to thwart their collective efforts. Otherwise, the efforts will be undermined, and the effectiveness will be limited.

"Isn't legislation to restrict spamming a violation of our charter right to Freedom of Speech?

Legislation that protects users from unsolicited commercial e-mail doesn't need to infringe on anyone's freedom of speech. It is important that those who are advertising at the expense of others are held to account for those costs or be forced to restrict their advertisements to those who are willing to bear those costs. It is about "consent, NOT content.

In the US the junk fax law was challenged in US court on First Amendment grounds and the court upheld the law because it is not censorship... it's about making the advertiser bear their own costs. The other US bills make the recipients bear the costs.

In the landmark case AOL vs Cyberpromo, this argument was also tried, and shot down.

The CRTC [fact sheet on Telemarketing](#) provides a list of specific rules that telemarketers must follow. Among them is the restriction of fax calls to daytime hours according to the timezone of the called party. Those sending faxes are also required to provide a valid mailing address, phone and fax number, and name of a responsible person to contact. Sequential dialing as well as dialing to healthcare and emergency facilities is forbidden. Each telemarketing organization is required to maintain and abide by DO NOT CALL lists. Telemarketers calling in person are not restricted to daytime hours but must, upon request, provide phone number, name and address of a responsible person as well as the name of the organization they represent.

CAUCE Canada lobbies for and supports legislation that requires commercial e-mail advertisers to act responsibly. Consumers have the right to clean mailboxes, the burden is placed squarely upon the advertiser to obtain permission from the recipient to send e-mail.” (<http://cauce.ca/faq.html>)

- The government could also consider the examples of several U.S. states that “have passed laws making it illegal to ‘sell, give, or otherwise distribute’ spamming software. Nevertheless, spamware is itself one of the classes of products more commonly advertised in spam” (Krueger). These spamware products engage in illicit activities to forge e-mail headers, exploit known vulnerabilities and open relays, and cover the track to evade detection. The promotion and distribution of such products should be restricted or even outlawed.
- The government could invest additional resources in law enforcement agencies to investigate and prosecute perpetrators who do not comply to the law. The combination of imposing hefty fines, and enforcing anti-spam legislations will sufficiently deter prospective mass marketers from indiscriminately spamming consumers.
- The government could study EU’s legal precedent as a model to curtail offshore spamming. Since spammers are not confined by national boundaries, and spam e-mail knows no border, any jurisdictions’ legislative initiatives to reduce spam will be undermined when spammers circumvent the law by moving their operations offshore. They can and will exploit international loopholes to achieve their objective.

“But the bigger problem is that a lot of spam originates in other countries, where Canada has no right to prosecute. European Union countries are strictly prohibited from doing business with countries that don't have an adequate level of data protection. Shouldn't we have the same restriction? "It's a tough 'Should we?' " Says Ms. Cavoukian, because there are economic repercussions. But she thinks consumers will increasingly demand it.” (Kerr)

“Yesterday's vote will turn Europe into a virtual "spam-free zone" after the formal adoption of the directive, making it illegal to send unsolicited e-mail, text message or other similar advertisements to individuals with whom companies do not have a preexisting business relationship.

"This is a tremendous day for European Internet users," said EuroCAUCE Chairman George Mills. "We are extremely pleased that the European Parliament has listened to the citizens of its member countries and added the right to be left alone by spammers to its efforts to protect the privacy of Europeans."

While six European Parliament member countries had already formalized "opt-in" in their national laws and regulations, yesterday's vote should turn all of Europe into a spam-free zone by the end of 2003.

"Unfortunately, the United States, Australia, Canada and India, as well as other countries in Asia, Africa, South America and elsewhere are now lagging behind Europe in their protection of Internet users," said CAUCE Chairman Scott Hazen Mueller. "This is a tremendous first step, but the rest of the world now needs to follow Europe's lead and unite behind protection of Internet users and network owners from abusive and costly unsolicited e-mail advertising."

(<http://www.cauce.org/pressreleases/20020531.shtml>)

- The above measures will re-balance the cost benefit equation of mass e-mailing. As marketers bear more of the costs, they will be more selective in their mail campaigns, and refrain from indiscriminate spamming of which the incremental cost is next to nothing. Consumers will have effective means to opt out of mailouts, and block spam based on distinctive header. They will burden less of the total costs, and they can regain the confidence in e-mail in particular, and the acceptance of the Internet and e-commerce in general.
- All stakeholders, including the ISP industry, software makers, consumer and consumer groups, the Internet community, marketers, and government jurisdictions, should collaborate the efforts together to address the issue of spam. The joint effort will facilitate roundtable discussion, exchange of ideas, and information dissemination. Specifically, the joint task force group will strategize, coordinate and implement an all-encompassing solution package.
 - The group could explore the idea of charging marketers “transmission cost” per e-mail. A Korean ISP is “charging commercial mailers sending bulk messages to more than 1,000 Daum account holders ten won (less than a penny) per message” (Chon). This strategy will move marketers from indiscriminate spamming to smarter “surgical strike” marketing of targeting prospective recipients.
 - The group could explore the idea of establishing a central registry of marketers and consumers. Marketers operating legitimate business can apply to be entered into the database, and pledge to adhere to self-policing guidelines. The consumer registry will consist of an “opt out” list of consumer addresses. Marketers will not send any e-mail to consumers

on the list. The registry administration body will form a self-regulating association, and clean up the image of marketers tarnished by the recent consumer backlash against spam. Also, consumers can elect to opt out of any mass e-mail advertisements, and complain to the body of any infractions.

- The group could initiate a consumer education campaign of e-mail etiquette. Part of the education is to help consumers to be aware of the seedy side of the Internet, protect themselves against potentially damaging spam tactics, and provide recourse when their rights are violated. Marketers should also be aware of the huge hidden costs of spamming. It is also to their benefits that they follow the guidelines to become responsible social and corporate citizens, which run legitimate business.
- ISPs should be encouraged to review and adhere to industry's best practices regarding Acceptable Use Policy (AUP) and spam (Hamsbridge and Lunde; Lindberg). For self-protection and cost reduction purposes, ISPs should rigorously exercise spam control on outbound messages, and install mail filters to screen inbound messages. ISPs could cooperate with the Internet community to produce a set of standard practices for maintaining, reporting, and querying blackhole lists. The lists serve as deterrents to rogue ISPs, which harbour known spammers.
- Software producers could seize the current market condition and capitalize it in developing new programs, which will aid in the fight against spam.
 - ◆ Develop more security-conscious software to protect PCs from being exploited as open relays and proxies.
 - ◆ Develop e-mail tracking software to facilitate law enforcement agencies in their investigative efforts.
 - ◆ Develop sophisticated mail filtering technology that is based on syntactical, lexicographical and contextual analysis of mail contents. One current product example of employing heuristic filtering is SpamAssassin.
- The group also can form a nation-wide lobbying group to advocate a spam-free environment and agenda to government officials. The lobbying group can provide a more balanced viewpoint on spam, and counter efforts by special interest groups to maintain the status quo in which spam roams freely and disruptively to Canadian households through the Internet.

Issues for further discussion

- E-mail Stalking. Last year, there was a groundbreaking criminal persecution of e-mail stalking in Canada. The case is believed to be the first of its kind in Canada, and was heard in Winnipeg (?). The female victim lives in Canada, and acquainted with a male friend in Europe several years ago. After a brief encounter, the relationship broke up, and the woman returned to Canada. However, the man pursued her, and stalked her through e-mail and other means. The man was arrested and persecuted by authority for stalking when he came to Canada to visit her. The man was found guilty and sentenced. This precedent illustrates that e-mail is a communication medium which illicit and criminal elements can and will leverage to achieve their goals.
- Cell Phone Spamming. Marketers will go to extremes to spread their advertisements, and the advent of technology has provided them with more and more avenues. With cell phones or handheld devices so commonplace in the society, spam has found new targets. The difference this time is that consumers will directly pay for spam as it will clog up their mailboxes, and they will have to use up valuable airtime to clean up.

“For now, most consumers seem resigned to wielding the delete button to separate spam from other messages they want. But the war has moved to a new front: cell phones. Rodney Joffe, a founder of Web host Genuity, whose current ventures include an e-mail-marketing company, was enjoying a performance of Riverdance in a Phoenix, Ariz., theater early last year when he got spammed via a text message — a promotion from a mortgage company — on his phone. Cell-phone providers typically charge their customers to receive e-mail. "So not only was I getting spammed, I was paying for it," fumes Joffe, 47. He slammed the offending marketer with a lawsuit, which he won at the trial level. (The mortgage company is appealing.) Several states have joined the fray. In September, California became the first state to ban spam to cell phones and pagers. "E-mail has been ruined by spam," says Joffe. "We've got to stop it before it ruins cell phones." With so many ways to serve it up, though, one thing is clear: spam — the good, the bad and the ugly — is on the menu to stay.” (Takeuchi Cullen)

- The spam phenomenon cries out for proactive actions by all stakeholders to protect consumers and technological advances so that they could be employed appropriately, and in their intended way.

Resource References

Business References

1. Alsop, Stewart. "Dubya's Tasty Spam Recipe." *Fortune*. November 25, 2002.
2. Anonymous. "780,000,000." *Washington Post*, page E02. February 24, 2003.
3. Anonymous. "How the FTC Is Policing Privacy." *BusinessWeek*. June 5, 2002. URL: http://www.businessweek.com/technology/content/jun2002/tc2002065_9287.htm
4. Anonymous. "Make e-mail polluters pay." *The Economist*. October 17, 2002.
5. Anonymous. "Study: Spam Cost U.S. Corporations \$8.9B." URL: <http://asia.news.yahoo.com/030103/ap/d7oaoec80.html>
6. Anonymous. "War of words, action on spam." *The Globe and Mail*. February 23, 2003.
7. Anonymous. "U.S. lawmaker seeks to criminalize spam: Unsolicited e-mail." *Financial Post*. February 20, 2003.
8. Associated Press. "Verizon Settles 'Spam' Case, Claims Victory Defendant Barred From Sending E-Mail." *Washington Post*, page E2. October 30, 2002.
9. Black, Jane. "Inside the Spammers' Arsenal." *BusinessWeek*. March 1, 2002. URL: http://www.businessweek.com/technology/content/mar2002/tc2002031_7541.htm
10. Black, Jane. "The High Price of Spam." *BusinessWeek*. March 1, 2002. URL: http://www.businessweek.com/technology/content/mar2002/tc2002031_8613.htm
11. Borland, John. "Spyware arms race accelerates." *The Globe and Mail*. February 24, 2003.
12. Branscum, Deborah. "Finding the Perfect Spam Catcher." *Fortune*. December 14, 2001.
13. Chon, Gina. "Making Spam Pay - Block that free e-mail." *Fortune*. April 15, 2002.
14. France, Mike. "Commentary: Needed Now: Laws to Can Spam." *BusinessWeek*. October 7, 2002. URL: http://www.businessweek.com/magazine/content/02_40/b3802104.htm and http://www.businessweek.com/smallbiz/content/sep2002/sb20020926_5958.htm
15. France, Mike. "Commentary: Needed Now: Laws to Can Spam." *BusinessWeek*. October 7, 2002. URL: http://www.businessweek.com/magazine/content/02_40/b3802104.htm and http://www.businessweek.com/smallbiz/content/sep2002/sb20020926_5958.htm
16. Grossman, Lev. "Send That E-Mail to Jail." *Time*. July 1, 2002.
17. Harrison, Laird. "You've Got Ads!" *Time*. January 14, 2002.
18. Klein, Karen E. "Making the Most of E-Mail Marketing." *BusinessWeek*. October 9, 2002. URL: http://www.businessweek.com/smallbiz/content/oct2002/sb2002109_8220.htm
19. Levy, Stephen. "How to Can the Spam." *Newsweek*. February 24, 2003.

20. Lidsky, David. "Forgiveness Marketing - E-mail marketing is broken." *Fortune*. July 31, 2002.
21. Lidsky, David. "Some Call It Trash - Spam blockers pull off a neat trick: They're worse than spam itself." *Fortune*. February 4, 2003.
22. McCullagh, Declan. "Consuming Spam Mail." February 12, 2001 . URL: <http://www.econlib.org/library/Columns/McCullaghspam.html>
23. McGuire, David. "Network Solutions Spills E-Mail Addresses." *Washington Post*, page E5. January 24, 2003.
24. Micek, John L. "U.S. Subcommittee Clears Landmark Anti-Spam Bill." *NewsFactor Network*. March 22, 2001. URL: <http://www.newsfactor.com/perl/story/8369.html>
25. Osterman, Michael. "Spam not at economic equilibrium." *Network World Messaging Newsletter*. February 11, 2003. URL: <http://www.nwfusion.com/newsletters/gwm/2003/0210msg1.html>
26. Pegoraro, Rob. "In E-Mail Software, the Medium Is the Mess." *Washington Post*, page H7. December 22, 2002.
27. Quittner, Joshua. "Can That Spam!" *Time*. June 1, 1998.
28. Rabinovitch, Eyal. "Essential Ad-Ons - Use this software to keep unwanted e-mail to a minimum." *Fortune*. September 30, 2002.
29. Salkever, Alex. "Strategies for Winning the War on Spam." *BusinessWeek*. August 20, 2002. URL: http://www.businessweek.com/technology/content/aug2002/tc20020820_1318.htm
30. Schuman, Evan. "Economic woes cause e-mail SPAM to soar." March 4, 2002. URL: <http://www.evanschuman.com/clips/upispam/upispam.html>
31. Seltzer, Larry. "PC Protection With No Fuss." *Fortune*. November 1, 2002.
32. Stone, Brad, Lin, Jennifer and Ulick, Josh. "Spamming the World." *Newsweek*. August 19, 2002.
33. Stone, Brad. "The New Spam Blockers." *Newsweek*. November 11, 2002.
34. Takeuchi Cullen, Lisa. "Some More Spam, Please ." *Time*. November 11, 2002.
35. Vise, David A. "AOL Joins Microsoft In a Reply to Spam." *Washington Post*, page E1. February 21, 2003.
36. Weston, Brendan. "Costly 'spam' flood soaks all office ranks." *Financial Post*. February 17, 2003.
37. Wildstrom, Stephen H. "Blocking Spam from Home." *BusinessWeek*. August 23, 2002. URL: http://www.businessweek.com/technology/content/aug2002/tc20020823_1111.htm
38. Wildstrom, Stephen H. "Can Anyone Put a Lid on Porno Spam." *BusinessWeek*. March 18, 2002. URL: http://www.businessweek.com/magazine/content/02_11/b3774025.htm
39. Wildstrom, Stephen H. "How to Control That Damn Spam." *BusinessWeek*. September 2, 2002. URL: http://www.businessweek.com/magazine/content/02_35/b3797025.htm

Technical References

1. Anonymous. "Offshore Bulk Hosting." The Spamhaus Project. November 12, 2001. URL: http://www.spamhaus.org/action.lasso?-database=sbl_news&-layout=detail&-response=newsstory.lasso&recordID=80&-search
2. Anonymous. "Spammers Grab MSN Hotmail Addresses." The Spamhaus Project. January 5, 2003. URL: http://www.spamhaus.org/action.lasso?-database=sbl_news&-layout=detail&-response=newsstory.lasso&recordID=114&-search
3. Anonymous. "The Problem." The Canadian CAUCE (Coalition Against Unsolicited Commercial Email). URL: <http://cauce.ca/about.html>
4. Bowman, Lisa M. "Consumer groups fight spam epidemic." Cnet News.com. September 3, 2002. URL: <http://news.com.com/2100-1023-956393.html>
5. Festa, Paul. "Microsoft going after Hotmail spammers." Cnet News.com. February 18, 2003. URL: <http://news.com.com/2100-1023-985018.html>
6. Festa, Paul. "Microsoft planning more spam suits." Cnet News.com. February 19, 2003. URL: <http://news.com.com/2100-1023-985215.html>
7. Festa, Paul. "Microsoft tries to cook Hotmail spammers." ZDnet. February 19, 2003. URL: <http://zdnet.com.com/2100-1104-985018.html>
8. Granato, John T. "You Got Mail – I Mean Spam!" SANS Institute Information Security Reading Room. March 14, 2001. URL: http://www.sans.org/rr/email/spam_battle.php
9. Hambridge, S. and Lunde, A. "DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*)." RFC 2635 and FYI0035, IETF Network Working Group. June 1999. URL: <ftp://ftp.rfc-editor.org/in-notes/rfc2635.txt>
10. Kane, Margaret. "Building a better spam trap." Cnet News.com. January 17, 2003. URL: <http://news.com.com/2100-1023-981177.html>
11. Kane, Margaret. "If it's spam, the message is 'delete'." Cnet News.com. August 29, 2002. URL: <http://news.com.com/2100-1017-955806.html>
12. Kontzer, Tony. "Anti-Spam Tool Is 'User Aware'." InformationWeek. June 6, 2002. <http://www.informationweek.com/story/IWK20020606S0014>
13. Kontzer, Tony. "Users Fight Back Against Spam Epidemic." InformationWeek. May 6, 2002. URL: <http://www.informationweek.com/story/IWK20020502S0008>
14. Krueger, Karl A. "The Spam Battle 2002: A Tactical Update" SANS Institute Information Security Reading Room. September 2002. URL: http://www.sans.org/rr/email/spam_battle.php

15. Lemos, Robert. "You've got spam, and more spam." Cnet News.com. August 29, 2002. URL: <http://news.com.com/2100-1001-955842.html>
16. Lindberg, G. "Anti-Spam Recommendations for SMTP MTAs." RFC 2505 and BCP0030, IETF Network Working Group. February 1999. URL: <ftp://ftp.rfc-editor.org/in-notes/rfc2505.txt>
17. McCullagh, Declan. "Groups seek federal action on spam." Cnet News.com. September 4, 2002. URL: <http://news.com.com/2100-1023-956502.html?tag=dd.ne.dht.nl-sty.0>
18. McCullagh, Declan. "Spam blocker charges for e-mail." Cnet News.com. February 19, 2003. URL: <http://news.com.com/2100-1023-985175.html>
19. Olsen, Stefanie. "AT&T spam filter loses valid e-mail." Cnet News.com. January 24, 2003. URL: <http://news.com.com/2100-1023-982118.html>
20. Olsen, Stefanie. "War of words, action on spam." Cnet News.com. February 20, 2003. URL: <http://news.com.com/2100-1023-985415.html>
21. Ramasubramanian, Suresh. "Spam Costs Everybody." URL: http://www.efuse.com/Grow/postage_due.html
22. Smith, Tom. "The Biggest Reasons Readers Hate Spam." InternetWeek. September 5, 2002. URL: <http://www.internetweek.com/story/INW20020905S0004>
23. Tran, Nam. "Anti Spamming – How to Filter Unsolicited e-mail on Your Mail Server" SANS Institute Information Security Reading Room. December 27, 2001. URL: http://www.sans.org/rr/email/spam_battle.php
24. Vanderlippe, John. "Block spam by any means." Cnet News.com. February 12, 2003. URL: <http://news.com.com/2009-1081-984317.html>
25. Wagner, Mitch. "ISP Chief: Spam Is 'A Thousand Times More Horrible Than You Can Imagine'." InternetWeek. December 19, 2002. URL: <http://www.internetweek.com/story/showArticle.jhtml?articleID=6400881>
26. Wagner, Mitch. "ISP Head Floats Plan To Legalize Spam." InternetWeek. February 20, 2003. URL: <http://www.internetweek.com/story/showArticle.jhtml?articleID=6900346>
27. Wagner, Mitch. "Spammers' Technology Secrets! Exposed!." InternetWeek. February 13, 2003. URL: <http://www.internetweek.com/story/showArticle.jhtml?articleID=6900020>

Government/Legal References

1. Anonymous. "Discussion Paper - E-mail marketing: Consumer choices and business opportunities." Industry Canada. January 2003. URL: http://e-com.ic.gc.ca/english/strat/email_marketing.html

2. Anonymous. "Global Community Applauds European Anti-Spam Vote." The CAUCE (Coalition Against Unsolicited Commercial Email). May 31, 2002. URL: <http://www.cauce.org/pressreleases/20020531.shtml>
3. Anonymous. "Internet and Bulk Unsolicited Electronic Mail (SPAM)." Industry Canada. July 1999. URL: <http://e-com.ic.gc.ca/english/strat/spam.html>
4. Anonymous. "Protecting Your Privacy on the Internet." The Privacy Commissioner of Canada. July 2001. URL: http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp
5. Anonymous. "Quick FAQ." The CAUCE (Coalition Against Unsolicited Commercial Email). May 31, 2002. URL: <http://cauce.ca/faq.html>
6. Anonymous. "Spam - Frequently Asked Questions." The National Office for the Information Economy (NOIE), Australia. URL: <http://www.noie.gov.au/projects/confidence/Improving/Spam/Info.htm>
7. Anonymous. "Spam Interim Review Report - Major Problems Caused by Spam." The National Office for the Information Economy (NOIE), Australia. URL: http://www.noie.gov.au/projects/confidence/Improving/Spam/Interim_Report/major_prob.htm
8. Anonymous. "Spam Review Interim Report." The National Office for the Information Economy (NOIE), Australia. URL: http://www.noie.gov.au/projects/confidence/Improving/Spam/Interim_Report/index.htm
9. Anonymous. "Statutes of Canada 2000." The Privacy Commissioner of Canada. URL: http://www.privcom.gc.ca/fs-fi/02_05_d_13_e.asp
10. Anonymous. "Washington State Supreme Court Upholds Constitutionality of State Anti-Spam Law, Overturns Lower-Court Rulings." The CAUCE (Coalition Against Unsolicited Commercial Email). June 7, 2001. URL: <http://www.cauce.org/pressreleases/washington.shtml>
11. Bennet, Chris. "Green Regs and Spam: Regulation of Unsolicited Commercial E-mail." Intelligence. Issue 2. URL: http://www.davis.ca/publications/2002-04_intelligence_april_2002.pdf
12. Breaux, John. "Canning Spam." May 18, 2001. URL: <http://www.senate.gov/member/la/breaux/general/columns/2001522830.html>
13. Geist, Michael. "Time to hit delete key on weak spam policy". The Globe and Mail. May 30, 2002. URL: www.globeandmail.com/servlet/ArticleNews/printarticle/gam/20020530/TWGEIS2 and <http://cauce.ca/spambygeist>
14. Kerr, Ann. "Still grey areas in new privacy law." The Globe and Mail. June 9, 2000. URL: <http://www.globetechnology.com/archive/gam/Specials/20000609/ECPEBR.html>
15. Munro, Eve. "Spam - Not Just a Luncheon Meat." For the Record. Winter 2000 Edition. URL: <http://www.swinton.ca/news/articles/fortherecord/winter2000/spam.htm>

16. W.K. Khong, “Spam Law for the Internet” (2001) *The Journal of Information, Law and Technology*.