Balancing Competing Interests: Managing And Regulating Spam While Preserving The Availability Of E-Mail For Ethical Commercial Users

Catherine S. Neal, (Email: nealc1@nku.edu), Northern Kentucky University
Douglas Havelka, (Email: havelkdj@muohio.edu), Miami University

ABSTRACT

A layered model composed of the legal environment, the network/service providers, the firm, and the individual is proposed for studying and managing unsolicited commercial email, i.e. spam.

INTRODUCTION

In the infamous Monty Python's Flying Circus "SPAM" skit, the term spam is used 87 times in the course of a two-minute sketch involving Vikings and breakfast food. The word spam accounts for 26% of the words in the skit. If only e-mail users were so fortunate. In a recent survey conducted by the Radicati Group, a California research firm, it was found that 49% of all e-mail sent globally in 2004 constituted unwanted spam (Hesseldahl). Teney Takahashi, an analyst with the Radicati Group, believes that in 2005, 73% of the e-mail messages consumers receive will be spam, as will be 48% of those received by businesses (Hesseldahl). Postini, Inc., an e-mail services company, estimates spam has increased by 65% since January 2002 (Chabrow). For businesses, the uninvited receipt of mass quantities of spam in company-provided inboxes significantly increased operating expenses over the past few years, and its presence will continue to impact the cost of doing business. It is estimated that $3 billion a year is spent on anti-spam technology ("Winning"). Worldwide, lost output attributed to the nuisance of spam is estimated at $50 billion ("Winning").

While consumers and companies burdened with the high cost and frustration of dealing with spam have been, and continue to be, very vocal about their hatred of unethical spammers, there are others who are concerned with the chilling effect this public outcry and recent legislation will have on those who legitimately transact business through the use of e-mail. Have spammers tarnished the use of e-mail as a legitimate marketing tool? Do anti-spam legislation and recent court cases strike a balance between regulating spam while leaving e-mail available to those who ethically transact business with its use?

WHAT IS SPAM?

Defining spam is one of the difficulties in combating it. During a taping of the *Charlie Rose Show* Microsoft chief counsel Brad Smith defined spam as "unsolicited commercial email sent to advertise a product or a service," AOL's senior vice president Joe Barrett called spam "an unwanted automated message," and FTC commissioner Orson Swindle coined the "Swindle Rule" by defining spam as "anything I don't like" (Berlind). Clearly, defining spam is difficult. What is unsolicited and unwanted to one person may be, to another, valuable information. This issue impacts the ability to deal effectively with spam because each individual user may wish to apply his or her own rules for managing spam. The fact that 45.8 million Americans (9% of all American e-mail users) made a purchase in the previous 12 months in response to an email advertisement, yielding $7.1 billion in sales, according to a study commissioned by the Direct Marketing Association, is evidence that unsolicited commercial e-mail is effective for some consumers and for some businesses ("DMA").

WHY DOES SPAMMING WORK?

One reason spam is ubiquitous is because it is so easy to become a spammer. In fact, spammers may include anyone who uses a mailing list to send out information in a bulk fashion electronically, e.g., a newsletter or monthly update to clients. However, the true culprits are those companies that or individuals who purchase or steal e-mail addresses by the millions and use those addresses as the targets for uninvited information. Often, these solicitations are offensive - - blatantly touting drugs, gambling, and products to enhance sexual performance. It is this use of e-mail that is viewed as unethical, and that has garnered the wrath of e-mail users, of government regulators, and now, the courts.

Spammers make money by playing a numbers game. They send out millions (literally millions) of e-mails everyday trying to get just a small percentage of responses to cover their bandwidth costs and negligible investment of time. Because creating and sending e-mail is inexpensive, spammers' modest expenses are quickly covered. The recent trial of Jeremy Jaynes in Leesburg, Virginia shows that by making $40 on one response to every 30,000 solicitations, Mr. Jaynes was able to make up to $750,000 per month ("Trial"). It is believed that Jaynes got his e-mail addresses from stolen data from AOL and eBay ("Trial").

Today, spammers themselves do not need to obtain and manage addresses to effectively spam. A query of any major search engines for the term "bulk email" will result in many web sites offering to send a message, for a small nominal fee of course, to millions of email subscribers. For example, see http://www.marketing-2000.net/, http://www.massmailsoftware.com/, http://www.lmhsoft.com/, and http://www.bulkemailsoft.com/, the first four result found with the search "bulk email" using http://google.com.

MANAGING SPAM

To stop the proliferation of spam and reduce the costs associated with it, proposed strategies should include both technical approaches and management policies. We propose a layered model for the management of spam by organizations. This model includes four layers of responsibility; the legal and regulatory environment, the network or service provider layer, the firm layer, and the individual layer. When combined, the strategies used at each layer form a coherent spam management policy.

Taking a top-down approach, the top layer of responsibility is the legal environment where state and federal governments can regulate spam. The second layer is at the email service provider where bulk traffic can impact communication costs. The third layer of responsibility is at the firm or organizational layer where spam is managed through policies and technological solutions. The lowest layer rests with individual users, i.e. actions that individuals should take to reduce exposure to spam.

The key to all these strategies is the tradeoff that must be made between blocking a high number of unwanted spam against the chance that "good" or "valid" legitimate email will get blocked because they have spam characteristics (this is called a *false-positive*). Currently, with the appropriate mix of policies and technologies companies can block roughly 90% of unwanted spam at an acceptable level of false-positives. To manage false-positives, users are able to view blocked messages in a "quarantine area" and the ability to add legitimate senders to a "whitelist" of trusted sources so that they will not be blocked in the future.

Also, it very important to test your anti-spam strategy prior to full implementation, especially if a high number of false positives could cost your company business. One approach to testing is to create "shadow" email accounts for some of the larger email users in your company and use your anti-spam strategy on these accounts and compare the number of correct blocks, false-positives, and email that should have been caught but were not (*false-negatives)* to determine how effective the strategy is working.

LAYER 1: THE LEGAL AND REGULATORY ENVIRONMENT

On December 8th, 2003 the U.S. Congress passed, and President Bush signed shortly thereafter, the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, known as the "CAN-SPAM Act of 2003," which is codified at 15 U.S.C. §§7701-7713, 18 U.S.C. §1037, 28 U.S.C. §994, and 47 U.S.C. §227. The law became effective on January 1, 2004 and preempts all the previously enacted state anti-spam laws. The provisions of the CAN-SPAM Act apply to any commercial electronic mail message, which the act defines as broadly as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)." This comprehensive piece of federal legislation creates a set of rules that bulk e-mailers must follow, including the requirements that bulk e-mailers provide an "opt-out" mechanism, a valid postal address in the e-mail, and labeling in the subject line for adult-oriented content only. Commercial e-mailers are prohibited from using deceptive subject lines or false return addresses and are prohibited from e-mail address harvesting, automated dictionary attacks, and routing disguising. The penalties for violating the provisions of the CAN-SPAM Act include fines of up to $6 million and prison terms up to five years. The stated purpose of the act is "[t]o regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet."

Even though the CAN-SPAM Act is a complex and comprehensive piece of legislation, the law has been criticized as not being tough enough, and of being difficult to enforce (Friel). Perhaps in response to such criticism, Congress directed the Federal Trade Commission, the federal administrative agency charged with enforcing the law, to consider restrictive regulatory mechanisms, most notably suggesting a "do-not-e-mail-registry," a device akin to the Federal Communications Commission's National "Do-Not-Call Registry," the restrictive regulation for which 60% of American consumers have subscribed, and which significantly contracts the world for telemarketers (and perhaps inadvertently encourages other means of mass marketing, like spam) (Booker). But, the FTC has thus far declined to institute a "do-not-e-mail" registry, and it does not appear that such restrictive regulation is necessary, especially considering the competing interests of ethical commercial users of e-mail.

First, the market, along with the current level of government regulation appears to be effectively reducing spam. America Online recently reported that spam complaints among the service-provider's members dropped by 85% over the past two years, and the number of spam messages AOL received each day dropped by nearly half during that same two year period (Chabrow).

In addition, the outcome of recent spam litigation will deter the most unethical of spammers. Scott Richter, known as the "spam king," recently agreed to pay $7 million to Microsoft in settlement of damages caused to the company by his unethical use of bulk e-mail. As part of the settlement agreement, Richter also agreed to stop sending unsolicited bulk e-mail (Chabrow). In other recent spam litigation, AOL was awarded $13 million dollars by a federal court (Chabrow). In concert with anti-spam law, these high-profile, big-dollar cases will undoubtedly deter similar bad actors, and accordingly, reduce the need for future government regulation of commercial e-mail use, leaving it available to those who ethically and legally use e-mail for commercial purposes.

LAYER 2: THE NETWORK OR SERVICE PROVIDERS' RESPONSE

One rule service providers use to block bulk spam an email is to watch for the same text in the subject line or in the message body in a large number of messages. To avoid blocking legitimate bulk emailings by newsletters, etc. the service providers began building *whitelists* of legitimate bulk email senders. Today spammers avoid this rule by inserting a randomly generated word into the subject line, and body, for every message sent. This is why you see text like "Make more money! dfjapf" in subject lines.

Another technique used by service providers, which can be used by in-house email servers also, is the use of IP address blacklists to filter spam. Spammers use email servers to send there messages. Every email server has an IP (Internet Protocol) address. There are several anti-spam organizations that maintain lists of IP addresses that are used by spammers; spamhaus.org is one of the best known and a leading force against spammers. Unfortunately,

spammers change their IP addresses frequently and the more aggressive spammers recruit "zombie" computers from unsuspecting Internet users to send their spam.

Honeypots are fake, but active, email accounts used by service providers and outsourcers to identify spam. By monitoring what messages get sent to these accounts and from where, bulk spam can be identified and potentially the source. Some service providers consider any messages sent to these accounts to be spam and block similar messages throughout their networks.

LAYER 3: FIRM APPROACHES TO MANAGING SPAM

For most businesses using a "cocktail" or mixed strategy to manage spam is appropriate. This implies using multiple techniques to reduce the costs of spam to the organization. In addition, it is strongly recommended that when implementing any new techniques that they be tested and implemented in a deliberate manner to avoid costs associated with false-positives.

One strategy for smaller organizations is outsourcing. Some service providers offer email services that include anti-spam filtering and individual customization. Besides the advantages of not purchasing and maintaining servers, outsourcing email services usually means quicker updates to anti-spam software and blacklists. The disadvantages include trusting an outside party to decide what email makes it through the filter and there are client privacy and confidentiality issues to consider since filtering implies that email content will be read. This may be unacceptable for some businesses, e.g. tax and audit clients.

Another strategy that is being used by organizations is to eliminate spam by eliminating email. Instead of using email software to receive communications from the outside world, some companies are now using online forms. This approach has its limitations, but it provides a means of delivering simple messages and may be appropriate for many business applications, e.g. students requesting information from a university or addressing a question to the admissions office. In addition, this approach could be used by businesses to help manage false-positives. For example, the FTC is attempting to reply to false-positives with a message that directs the sender to a web site that contains an on-line form. This way, legitimate senders whose email has been rejected by the filtering software can still get a message to someone at the FTC.

Other measures to manage spam include:

- Educate your employees regarding company email policies and how to avoid spam.
- Establish an email address (or on-line form) for employees to report spam to the IT department.
- Conduct occasional audits of blocked messages to manage the rate of false-positives.

LAYER 4: INDIVIDUAL ACTIONS

There are several good rules of thumb to follow and technology solutions available to help you, as an individual, avoid receiving spam or to reduce the costs and consequences of spam. A set of these rules are given in Table 1 below and some of the associated techniques are discussed in the following section.

Plus-addressing. One way to determine who is giving out your email address to spammers is by using *plus-addressing*, which is available from several free email services. Plus-addressing allows you to obtain a basic email address, e.g. doug@muohio.edu, and also provides a series of additional addresses, i.e. doug1@muohio.edu, doug2@muohio.edu, etc. When registering online for content or services, you use one of the plus-addresses. By tracking which address you use when registering and where spam shows up, you can pinpoint who is selling your email address.

Use dummy email addresses, multiple addresses for different purposes, change addresses as often as needed. Avoid registering software or other products that require an email address or use a free email address from Hotmail or

Yahoo for all of these types of communications. Consider using separate email accounts for friends and family, business, and all other messages. Abandon email addresses that become overwhelmed with spam.

Never reply to spam. By replying you are confirming that your email address is active. This includes clicking any unsubscribe link. Also, you should avoid buying products or services from spam email. This reduces the monetary incentive to spam and that is what most spammers are about and your purchase helps to finance them.

Use the spam filters provided by your email software or be sure that your email service provider is using adequate filtering techniques. Report repeating spam to your ISP (you can also report spam to the FTC at "uce@ftc.gov").

Do not use the preview pane in your email package. By using this feature you may automatically report back to the spammer that your account is active and valid.

Do not publish your email address on a website. If you do, do not make it a hot link. This reduces the likelihood that a spider will find it. You may also want to disguise the address so that a program is unlikely to understand it, but a human would. For example, I might use "doug @ muohio.edu" with the extra spaces and quotation marks knowing that a human reader would know to delete these when sending a message.

Be certain to use virus protection and firewalls to protect your machine from being used by spammers as a zombie.

If you receive spam that promotes well-known or respectable brands, complain to the company about its use of spam. It may be more effective to do this through traditional methods, i.e. the U.S. post office.

If you choose to register for information or content on the web, be sure to uncheck boxes that are set to "opt you in" to mailings from the source and their "partners."

Do not forward chain letters, petitions, or virus warnings from sources you do not trust. These have been used by spammers to collect addresses.

CONCLUSION

Spam costs business real money in terms of the human and technological resources required to deal with an increased volume of e-mail. But, by adopting a multi-layered technical and management approach, organizations can minimize the negative impact of spam without the need for additional government regulation of commercial e-mail, leaving e-mail available for ethical commercial users.

Table 1 – Individual Rules To Avoid Spam

1.	Guard Your In-Box
2.	Use Free Web Mail Accounts
3.	Use a Disposable E-mail Address
4.	Use Fake Addresses
5.	Don't Post Your Address
6.	Don't Answer Spam. Ever.
7.	Opt-Out & Don't Opt-In
8.	Read the Privacy Policy
9.	Don't View Spam Messages in your In-Box
10.	Use Email Filtering Software
11.	Forward Deceptive Email to the Feds (uce@ftc.gov)

REFERENCES

1. Berlind, David, The biggest spam challenge: defining it, *Tech Update*, August 28, 2003.
2. Booker, Ellis, Direct marketing in the shadow of privacy concerns, legislation, *B to B,* August 8, 2005, Vol. 90, Issue 10.
3. Chabrow, Eric, In the Fight Against Spam, A Few Knockouts, *Information Week,* August 15, 2005, Issue 1052.
4. DMA tells house: e-mail marketing is boon to small businesses, *DMA Press Release*, October 20, 2003. http://www.the-dma.org/cgi.
5. Friel, Alan L., The Spam Spat: How will marketers be affected by the fight against spam? *Marketing Management,* May/June 2005, Vol. 14, Issue 3.
6. National Do Not Call Registry, https://www.donotcall.gov/
7. Trial shows how spammers operate, *Associated Press*, November 15, 2004, http://www.msnbc.msn.com/id/6492244/
8. Winning the war on spam: Unwanted e-mails are no longer the menace they once were, *The Economist*, August 20, 2005, Volume 376, Issue 8440.