# Spam 2005:
# Technology, Law and Policy

Center for Democracy & Technology
Washington D.C.

March 2005

The Center for Democracy & Technology is a non-profit, non-partisan public interest organization dedicated to developing and implementing public policies to protect and advance civil liberties and democratic values on the Internet.

Cover artwork was generated from spam messages received by the CDT webmaster in February 2005.

1634 I Street, NW Suite 1100
Washington DC 20006
(202) 637-9800
(202) 637-0968 (fax)
http://www.cdt.org

# Table of Contents

# Introduction

The Center for Democracy and Technology is pleased to present this compendium of papers, "Spam 2005: Technology, Law and Policy."

Passage of the CAN-SPAM Act in late 2003 marked an important milestone in the effort to stem the flow of unwanted, unsolicited commercial email. The law, which went into effect on January 1, 2004, codified minimum requirements for responsible email practices that, coupled with criminal sanctions, were intended to make it possible for law enforcement to identify and prosecute purveyors of spam.

Even as policymakers drafted the legislation, they acknowledged that the CAN-SPAM Act would serve at best as only a partial solution to the spam problem. Indeed, analysts have estimated that in 2004 spam comprised 77% of the messages users found in their email boxes. Strong anti-spam technologies and email users educated about how to avoid online behavior that encourages spammers are also keys to addressing spam.

In recent months, attention has turned to the development of technological measures that lessen the flow of spam closer to its source. While anti-spam measures have traditionally filtered spam at the point of delivery, emerging technologies seek to recognize and stop spam at an earlier point in the email system, alleviating the burden of spam for both recipients and Internet service providers.

These technological developments represent a positive and powerful step forward in the effort to reduce spam, but they also raise fundamental issues about how the Internet should work: To what extent will anti-spam technologies pose barriers to access to this inexpensive medium? On the basis of what criteria will ISPs, assisted by these technologies, decide what email will be delivered? Will anti-spam technologies continue to accommodate anonymous political speech? What will be the impact of these developments on non-profit organizations?

The papers in this compendium attempt to present a snapshot of the current conversation about spam. Some of the papers assess the status of the spam problem and the efforts of law enforcement to use the CAN-SPAM law. Two writers from the European Union offer analysis and perspective about how the problem of spam is addressed through the EU Directive, and why that approach is preferred in Europe. The compendium also includes papers by companies promoting technologies, sometimes coupled with policies and best practices, offering spam solutions to consumers and to businesses. Finally, the compendium offers the perspective of a civil libertarian and a non-governmental organization on the impact of anti-spam efforts on free expression and political speech.

In compiling these papers, we attempted as much as possible to be inclusive and balanced. However, the complexity of the problem and the wide range of solutions under development necessitates that this document is limited in scope. What the compendium does endeavor to do is offer a thoughtful look at the spam problem, efforts to address spam through law both in the US and abroad, and some of the technologies under consideration and the issues they raise.

The result is a compendium that we hope will help to inform the ongoing discussion about how to reduce spam in a manner that best serves consumers, businesses, and ISPs. We hope that it will highlight the importance of addressing this problem in a manner that respects and preserves the vision of the Internet and email as media that promote democratic values and free expression.

We are grateful to the contributors to this compendium and look forward to participating in this inquiry as efforts to reduce spam continue.

Paula J. Bruening
Staff Counsel and Compendium Editor

# Section I - The Problem of Spam

# Spam: A Survey Review of the User Experience

*Deborah Fallows, Senior Research Fellow*
*Pew Internet & American Life Project*
*dfallows -at- pewinternet.org*

## Introduction

The huge increase in the volume of spam email over the last few years has taken a toll on the online world. Nearly a third of email users (29%) say they use electronic mail less now because of spam. Over twice that number (62%) say they trust the online environment less because of spam. More than three quarters of email users (77%) say that spam has made being online unpleasant or annoying. Overall, 86% of email users reported some level of distress from spam. Taken together, these data suggest that spam is undermining the integrity of email and degrading the online experience.

The figures cited in this paper represent the results of two national surveys of Internet users' awareness, behavior, and attitudes about email and spam, conducted by the Pew Internet & American Life Project. The first survey[1] was carried out in June, 2003, about 6 months before the CAN-SPAM Act went into effect. The second survey,[2] a shorter follow-up posing many of the same questions, was conducted 1 – 2 months after the CAN-SPAM Act went into effect in January 2004.

## Why Internet Users are Losing Trust in Email, and Why Some are Turning Away From It

Internet users offer several reasons why they are losing trust in email. Many report that they fear that genuine email, both incoming (30%) and outgoing (23%), is being caught up and lost by overly aggressive spam filters. Others worry they will simply overlook bona fide email amidst the growing clutter of spam in their inboxes; a full 29% say they are concerned they might accidentally delete an important email, mistaking it for spam.

Most email users express concern, as well, about the content and nature of the spam that arrives in their inboxes. These uninvited messages, they say, are deceptive and often disgusting. Some 80% of email users are bothered by the deceptive or dishonest content of spam; 76% are bothered by the offensive and obscene nature of some of it.

Both loss of trust in email and growth of the spam burden are beginning to drive some users away from email altogether. Over 4000 email users documented their personal experiences with spam[3], and many admitted the cost of spam is beginning to outweigh the benefit of email. One email user wrote, "Spam has 100% shut me and my family down. We can no longer deal with downloading one hour's worth of spam and viruses to get a message or two that we are expecting." And another echoes, "My time is valuable and I do not have time to filter through all this unwanted spam. So half the time I just hit 'select all' and delete every email I get. I have gone so far as to tell everyone not to bother emailing me. I have gone back to using the phone and no longer email anyone."

Others, primarily small business people for whom email is mission-critical to their livelihood, describe how they are held hostage by spam and forced to pick through spam in a painstaking and costly way. One, for example, writes, "I have been in business since 1994, and I cannot change my email address for business reasons. Currently, I average well over 50 unsolicited junk emails for every legitimate inquiry or comment from my customers. It is easy to overlook contacts from my users in all of the junk. I'm sure that this has cost me business from time to time but I'll never know because potential customer queries, almost always from people I do not know, are lost in the spam."

1. <http://www.pewinternet.org/pdfs/PIP_Spam_Report.pdf>.

2. <http://www.pewinternet.org/pdfs/PIP_Data_Memo_on_Spam.pdf>.

3. More than 4000 first-person narratives about spam were solicited since September, 2002, by the Telecommunications Research & Action Center (TRAC), a national consumer group. They shared these narratives with the Pew Internet & American Life Project.

## The Special Case of Pornographic Spam

By every measure, email users' reactions to spam containing adult content and pornography were most dramatic. Nearly four times as many email users identified pornography as more bothersome than any other kind of spam. Not surprisingly, women are significantly more troubled by pornographic spam than men (63% v. 42%), and parents are more troubled than non-parents (59% v. 49%). Some 71% of email users report that they have received pornographic spam.

Many emailers described their despair about the nature of the messages they receive and their sense of helplessness to do anything about it.

One wrote, "I am a grade 8 homeroom teacher. About midway through last school year, I started receiving an ever-increasing flow of spam – some of it absolutely inappropriate for a school environment. I'm receiving from 5 – 10 obscene spams each day, and I have to shoo my students away from my desk every time I check my email. Thus, my students are losing out from what used to be 'quality time' around my desk."

And another wrote, "You have no idea of how embarrassing it is for a priest to go 'online' to check his email...especially with others around...and find a barrage of pornographic messages on his computer. This happens to me all the time."

Some good news was reported between 1 – 2 months after the CAN-SPAM Act went into effect: 25% of email users say they were getting less pornographic spam than before January 1, 2004. Most people (56%), however, said they saw no change, and 16% saw increases in incoming pornographic spam.[4]

4. This good news appears in sharp contrast to other trends unfolding during the eight months between surveys. While about half of users reported their volume of spam was unchanged (53%), more reported an increase in spam than a decrease. In personal email accounts, 24% reported an increase in volume of spam and 20% reported a decrease; in work email accounts, 19% reported an increase in volume of spam and 11% reported a decrease. Further, there was a 4% increase in the number of email users who said they were cutting down on email use because of spam, an 11% increase of those who said they were losing trust in email because of spam, and a 7% increase of those who said spam made life online unpleasant or annoying.

## The Elusive Definition of Spam

Confounding and complicating the writing of effective and enforceable legislation against spam is the definition of spam. In the Spring of 2003, the Federal Trade Commission sponsored a three-day forum, comprehensively addressing every issue related to spam from economics to legislation, from technology to best practices. The opening morning was dominated by a lively and often heated debate over the definition of spam, but one that failed to reach consensus. When Internet users reponding to the spam survey were asked what they consider to be spam, they easily agreed on a basic definition, but one that quickly blurred at the edges. Some 92% of emailers agree that spam is "unsolicited commercial email from a sender they do not know or cannot identify." There is less agreement on other qualifying factors.

Emailers say that the content of the email matters. Some 92% consider unsolicited messages containing adult content to be spam. Then, 89% consider unsolicited investment deals, financial offers, or money-making proposals to be spam. Further, 81% consider unsolicited product or services to be spam. Beyond that, agreement drops off. Some 76% of emailers consider unsolicited email with political or religious messages to be spam.

Americans also believe that the relationship between the emailer and the sender matters. With commercial emails, prior relationships with the business matter most; over 90% consider email from senders with whom they have no prior relationship to be spam, while only about one third of emailers (32%) consider unsolicited emails from a sender with whom they've already done business to be spam. However, a stalwart few remain standing; 11% insist that unsolicited commercial email be considered spam even if they have given the sender permission to contact them. Although still largely considered spam, unsolicited messages from senders outside the world of commerce are more likely to be tolerated: "only" 74% of emailers consider unsolicited messages from political or advocacy groups to be spam; 65% consider unsolicited emails from nonprofits or charities to be spam.

## What Email Users Do with Their Spam

Many email users believe they know how to behave in a spam-saturated environment. But in fact, while some behaviors are appropriate, others backfire. Most email users take sensible and simple precautions against receiving spam: almost three quarters avoid giving our their email addresses (73%) and posting their addresses on the web (69%). Most immediately "click to delete" their incoming spam (86%).

Many others take actions that also seem reasonable, but in fact can be costly. Two-thirds of email users have clicked on a link within an unsolicited email to request to be removed from future mailings. This seemingly sensible action often sets off a maelstrom of incoming spam. Why? The FTC has reported that 63% of "remove me" requests were ignored by senders, and others suspect clicking the button only serves to confirm to a malicious spammer that he has found a live email address.

Other email users keep the spam industry in business: a full third of email users have clicked on a link within an email to get more information. More significantly, between 5% - 7% of email users report that they have ordered a product or service that was offered in an unsolicited email. And 9% say they had responded to an email offer only to discover later it was phony or fraudulent. Finally, 3% said they had provided personal information requested through an unsolicited email.

Using filters or services to deflect spam from arriving in inboxes is more common and more effective in workplace accounts than personal accounts. Some 62% of workers say their employers use filters to block spam from their email accounts, and nearly twice as many workers with those filters than those without report that they get no spam at all. By contrast, only 37% of individuals say they apply filters to their personal email accounts, and there is barely a difference in the amount of incoming spam reported by those who apply their own filters and those who do not.

Many email users wrote about the Catch-22 of fighting spam with filters. One writes typically, "I have finally managed spam to a point with which I can deal. First I always create a new email alias when communicating with an online service. Secondly, I run a program on my mail server which filters out just about all the spam. And, finally, I report spam to uce@ftc.gov and spamcop.org. The down side to this is that it takes too much time for what gets accomplished. I spend time no matter what – either deleting spam, or building and maintaining a defensive system."

## Implications of the Survey Findings

First, by nearly every measure, pornography soared to the top as the most offensive, objectionable, destructive type of spam. So extreme was the reaction that eliminating it alone among all unsolicited email would likely go a long way toward softening spam's negative impact on Internet users.

Second, we were struck by the extent to which Internet users' avail themselves of the simplest, most obvious solutions in their own confrontations with spam. In identifying spam, they looked at the subject and sender lines. In dealing with spam, they clicked "delete." In trying to avoid spam, they would do less rather than more on the Internet. This suggests that the most effective solutions will be simple ones that Internet users can and will employ.

And finally, there is the issue of trust. Time and time again in our surveys and reports on the Internet, Pew has found that trust is the backbone to making the most of the Internet. Web sites look for ways to convey trust. Consumers must trust transactions carried out on the web. And in the case of email, users need to trust that their email is legitimate, that it is reliably delivered or received, and that actions they take against unsolicited email, like clicking the "remove me" button, will actually return the promised result. The particular challenge with spam is that addressing problems through technology or legislation is just the beginning of an effective – and trustworthy – solution.

# Impact of Spam - Humana Business Perspective

*Beth Schowalter, Consumer Security Incident Response Technology Manager*
*Humana, Inc.*
*http://www.humana.com*

## Introduction

This paper focuses on the impact of spam on business communication efforts. This does not mean that spam does not impact other areas. Findings indicate spam's impact on an organization's ability to effectively deliver consumer communications while fighting the spam problem internally.

Businesses often consider spam sent to employees an annoyance, and rarely regard it as a serious problem that must be addressed systematically. While deleting unsolicited email takes only seconds, the failure to investigate the economic impact of spam has contributed to the underestimation of the problem it presents.

Properly functioning email systems allow businesses to effectively eliminate loss of customers and mitigate extensive and costly paper-based transactions. The proliferation of spam jeopardizes a company's ability to take advantage of these opportunities afforded by email technology. As a result, organizations are forced to implement anti-spam solutions to facilitate distribution of mission-critical email communications to consumers.

## About Humana

Humana Inc., headquartered in Louisville, Kentucky, is one of the nation's largest publicly traded health benefits companies, with approximately 7 million medical members located primarily in 15 states and Puerto Rico. Humana offers coordinated health insurance coverage and related services — through traditional and Internet-based plans — to employer groups, government-sponsored plans and individuals.

Humana has proven over its 43-year history that it embraces change. It has seized opportunities that have helped to transform its business.

Today, innovation serves Humana's efforts to transform its business to provide customers with personalized, actionable health benefits information in real time. With the right blend of product designs and the use of digital technology to achieve administrative simplicity for employer groups, physicians, hospitals and other health care providers, Humana is poised to take advantage of the tremendous opportunity offered by the growth of information technology.

## Incidence of Spam

Since April 2003, Humana has dealt with the proliferation of spam for its over 14,000 associates. The sheer volume of spam that evades anti-spam solutions has increased dramatically over time. Regardless of the effectiveness of spam quarantine solutions, a significant percentage of spam continues to be delivered. Estimates indicate approximately 11-15% of spam continues to reach associates regardless of our efforts to combat the problem. The numbers below, therefore, represent an estimate of the amount of quarantined spam.

Pieces of Spam:

| | **2003** | **2004** |
|---|---|---|
| Effectively quarantined | 12,299,928 | 60,762,676 |
| Estimated to have been delivered to associates | 1,844,989 | 7,233,345 |
| Delivered daily | 82,000 | 154,640 |
| Delivered hourly | 3,416 | 6,443 |

Increases of this nature reflect several shifts in trends, however. Before considering those trends it is important to note that spammers make money delivering email; they are diligent, effective and understand the architecture of email systems better than most. Spammers locate, evaluate, decode and defeat anti-spam solutions. They continue to win the spam war regardless of our efforts or the advances in anti spam solutions.

Humana has seen several shifts in trends over the course of the last two years, that include, but are not limited to:

- chain letters
- pyramid schemes
- get-rich-quick promotions
- advertisements for phone sex and ads for pornographic web sites
- offers for software
- stock offerings
- health products

More recently, spam has introduced into users email boxes:

- illegally pirated software
- spyware, adware
- keyloggers
- password grabbers
- phishing schemes
- proliferation of viruses
- trojans, worms and botnets

Spam is no longer merely annoying, it is now destructive to users' computers.

Spam poses substantial costs for organizations like Humana. Some experts advise that it takes one second to delete a single piece of spam. Determining whether a piece of email has been wrongly characterized as spam could take upwards of 4.4 seconds per piece of spam. These numbers suggest that Humana spent upwards of 2,255 hours deleting spam during 2003 and over 8,840 hours deleting spam during 2004, an increase of over 292% in 12 months.

## Damages, Costs and Productivity

Spam imposes significant costs on business. In addition to the costs of employing anti-spam solutions themselves, spam increases administrative costs associated with maintaining the technology.

Humana continues to deal with lost productivity caused by spam. Associates arrive at work each morning to find email files full of spam and spend the first 5 minutes of each day – collectively roughly 1200 hours - sorting, deleting and reporting what was delivered after the associate left work the day before. Spam frustrates associates and affects their ability to do their job effectively.

Spam delays mail servers, slowing the delivery of often time-sensitive legitimate business mail. Associated costs of spam include cluttered mail servers, increased costs associated with storage and backups, and costs related to hardware failures.

The most serious issues involve the workstations. Opening one piece of spam can cause hard drives to fail and require technical support staff to rebuild or replace the workstation, resulting in lost productivity and compromised customer service.

## Impact of the CAN-SPAM Act

Implementation of the CAN-SPAM Act of 2003 appears to have caused several things to happen over the course of the last year.

Because the legislation only applies to the United States, spammers have moved overseas or used overseas accounts to proliferate spam, seriously impeding our ability to find, investigate and prosecute spammers.

Since the CAN-SPAM Act was enacted, Humana experienced an increase in spam of roughly 494%. This suggests even US-based spammers ignore the law. In spite of publicized prosecution efforts, the problem is getting worse.

The volume of spam prompts consumers to employ anti-spam services. These tools often inadvertently quarantine legitimate Humana mail as spam, jeopardizing our ability to effectively communicate with our customers.

The effectiveness of marketing and communicating has drastically changed in the last 12 months because of the proliferation of spam. Organizations are being forced to use the same techniques as those who send spam in learning how to beat the spam filters in order to communicate with consumers. Electronic communication reduces our costs and allows us to leverage technology and transform the company's business to give our customers personalized, actionable health benefits information in real time.

The most important aspect we have yet to mention is the lack of confidence consumers have in electronic communications because of spam. The same issues we have seen and previously addressed are happening to consumers. They are not willing to accept email nor do they trust receiving it. This restricts our ability as an organization to effectively communicate with our consumers and will in the future raise serious cost shifting challenges.

## How Can We Effectively Deal With the Issue?

Understanding the problems and issues is the first step in developing a solution.

Legislation must be strengthened, upheld and enforced. Law enforcement must work with businesses to help them identify the source of spam and to prosecute spammers. Businesses need to work with government to enhance the current legislation. Legislation must be federal, it must pre-empt state law, and it must be technology neutral.

Broadening the legislative efforts overseas, however, requires aggressive prosecution. Penalties and fines that are actually enforced may deter spam activity.

Government, business and consumer advocates must engage in consumer awareness campaigns that enlist media support. A recent published survey indicated that approximately 46% of email marketing companies were not aware of the CAN-SPAM Act.

Government needs to find the “deep pockets”- those organizations spending the money to send spam. They need to get to the data centers that are processing the spam and shut them down or enhance the legislation to include the distribution centers. Once spammers are identified and prosecuted, we may find a reduction in this problem.

## Conclusion

Fighting this battle is no easy task, but one that must be undertaken. Ferris Research estimated the damage caused by spam at 8.9 billion USD and around 2.5 billion USD for European companies. The damage for U.S. and European ISPs (Internet Service Providers) is estimated to be around 500 million USD. Assuming the cost to delete emails by associates is 4.4 seconds work per spam mail, you can add yet another 4 billion USD annual loss of productivity for U.S. companies.

A solution is needed and enhanced legislation is required. We must increase awareness and consumers and business must join forces with the government to find a solution to this issue if we are to realize the benefits of email technology for companies and their customers.

# Section Two - Technological Responses

# A Multi-Pronged Approach to Eliminating Spam Email and Online Fraud

*Ryan Hamlin, General Manager, Safety Technology and Strategy Group*
*Microsoft Corp.*
*http://www.microsoft.com/spam*

Email is an essential tool for businesses, government agencies, organizations and individuals. Its value is being eroded, however, by the torrent of spam – unsolicited commercial email – clogging users' inboxes and straining corporate IT systems.

Consider the following:

- An estimated 65 percent of all email messages are spam.[1]
- The daily volume of junk emails sent worldwide is expected to reach 58 billion by the end of 2004, costing businesses $198 billion annually in software costs and lost productivity.[2]
- 63 percent of U.S. email users say spam makes them less trusting of email, an 11 percent increase compared to June 2003.[3]

Beyond email users' obvious and growing frustration with this epidemic, spam poses significant threats to computer security as a carrier of viruses and worms and as a channel for fraud. Many spammers employ deceptive practices such as "phishing" and "spoofing" to perpetrate scams aimed at stealing email recipients' sensitive personal information and financial assets. In a phishing scheme, the spammer crafts an email that appears to come from a legitimate and trusted source, such as the recipient's bank or an e-commerce merchant. The sender's email address is typically faked to appear legitimate, and the spam message often contains a link to an official-looking Web site – practices known as "spoofing" – so as to trick recipients into revealing credit card numbers, account passwords, Social Security numbers and similar personal information that can be used to commit identity theft and to engage in other illegal activities.

Spammers and phishers continue to find new ways to compromise the security, integrity and viability of the Internet and email, thereby undermining users' trust and confidence. The scourge of unwanted and malicious email is being driven by three powerful motivating factors:

- *Low cost of entry*. A spammer operating a handful of personal computers can send millions of email messages per day. Spammers also have many inexpensive ways to compile lists of recipients. The most common include bombarding email servers with millions of hypothetical addresses and tracking which ones will accept mail; using software that "scrapes" addresses from Web sites; and buying lists from other spammers or obtaining them from public sources.
- *High potential for lucrative returns*. If even one in 100,000 recipients responds to a spam email or phishing scam, the perpetrator is extremely successful. Some spammers claim to have reaped as much as $30,000 to $40,000 in a single month for minimal effort.
- *Anonymity*. Spammers employ a host of technologies and techniques to cover their tracks, from spoofing the source address to infecting an email recipient's computer with a worm or other malicious code that allows the spammer to send messages from the victim's email box.

The interplay of these factors dictates that an effective strategy for cracking down on spam and phishing focus on two key objectives: placing greater economic burdens on those who perpetrate these schemes, and enabling those who receive email reliably to authenticate the sender's identity and show evidence of good sending behavior. These ambitious goals, and the pervasive threats posed by malicious email, require a far more comprehensive array of countermeasures than either the government or the technology industry can mount independently. Technology companies, IT think tanks, government agencies and consumers must continue working together to overcome spam through a multi-pronged approach

1. Brightmail, Inc. (since acquired by Symantec Corp.), 2004.
2. The Radicati Group, 2003.
3. The Pew Internet & American Life Project, from a survey conducted between February 3 and March 1, 2004.

that encompasses technology innovation, industry collaboration, consumer education, strong legislation and aggressive law enforcement.

# Technology

Advances in spam email filtering technology have made spamming a more difficult and less rewarding business in recent years. Yet spammers persevere, sending ever-greater volumes of email and adopting more sophisticated methods of escaping detection by filters. Microsoft's anti-spam technical vision includes a distributed system of interconnected technologies and services to help prevent and protect against spam intrusions at key choke points on the network. This vision is built upon technologies that center on "the three Ps" of spam containment: proof of the sender's identity and evidence of responsible email sending practices; protection against spam attacks through effective filtering tools that distinguish spam from legitimate email; and prevention of spamming and phishing intrusions before they even reach organizational networks or users' computers.

## Authentication Technologies

While all three interconnected technology approaches are important, proof of identity and the ability to authenticate the origins of incoming email are vital to enable other anti-spam and anti-phishing efforts to function effectively. While authentication by itself will not stop spam, it lays the foundation for advanced technologies that are "smarter" about deciding which emails may pass through organizations' and end users' protective and preventative defenses. Moreover, the benefits of stronger authentication measures extend beyond the technology realm. Making email senders' true identities more transparent will lead to more effective and targeted enforcement of anti-spam laws by spotlighting offenders. It will also provide the basis for more widespread and well-informed cooperation among technology vendors, Internet service providers and others in the industry and help end users make better-informed decisions as they manage their email interactions.

Emerging email authentication mechanisms include Internet protocol address (IP)-based approaches like the Sender ID Framework (SIDF), which are a strategic first step for all businesses and email senders to embrace. Today nearly 200,000 domains have published their records to counter email forgeries and spoofing. Complementing SIDF is the promise of signing solutions with leading proposals from Cisco and Yahoo!. While these approaches differ in some key respects, both are vital to helping make spam and phishing emails easier to identify by providing a mechanism to verify the domains from which email is sent.

## Sender ID Framework

Sender ID Framework (SIDF) is a combination of Sender Policy Framework (SPF)[4] and the Microsoft Caller ID for Email draft proposals that have evolved over the past several months with important input from the MARID[5] working group of the Internet Engineering Task Force and a number of industry stakeholders.

Sender ID seeks to verify that every email message originates from the Internet domain from which it claims to have been sent. This is accomplished by checking the address of the server sending the mail against a registered list of servers that the domain owner or administrator has allowed to send email. This comparison is automatically performed by the Internet service provider (ISP) or recipient's mail server before the email message is delivered. If the check fails, the message is further analyzed and may be refused by the receiving server, or flagged to the user as a possible deceptive message. Depending on the recipient's ISP or email server software, messages that fail the Sender ID check may be flagged and sorted differently. For instance, a simple icon may be displayed within the message to indicate the failure; the message may be sent to the junk mail folder for the recipient's review; or it may be automatically rejected and deleted.

SIDF has been enhanced to provide deployment flexibility as well as to accommodate a combination of platform, application and licensing choices. This includes backward compatibility to the more than

4. SPF is a system that fights return path address forgery and makes it easier to identify spoofs. Domains use public records (DNS) to direct requests for different services (web, email, etc.) to the machines that perform these services. All domains publish email records to tell the world what machines receive mail for the domain. SPF works by domains publishing reverse records to tell the world what machines send mail from the domain. When receiving a message from a domain, the recipient can check those records to make sure mail is coming from where it should*.

5. MARID refers to MTA Authorization Records in DNS, formerly a working group of the Internet Engineering Task Force. See <http://www.ietf.org/html.charters/OLD/marid-charter.html>.

200,000 domains that have already published SPF records.

The SIDF and signature-based identity mechanisms also enable reputation and safe-list email accreditation systems, such as IronPort Systems Inc. and TRUSTe's Bonded Sender program, which can help filters make more informed decisions based on the email behavior patterns of the sender. These systems reward identifiably "good" email senders who adhere to stringent best practices and allow filtering technology to focus more closely on mail from non-accredited sources.

In addition, Microsoft is investigating new ways to help smaller-volume email senders and consumers easily provide evidence of good behavior. These include client-side computational puzzles that require computers to perform a complex calculation as part of the process of sending email messages, as the time involved in doing so makes sending bulk email much more difficult and serves as a deterrent to spammers. Proof approaches ultimately help reduce the financial incentive for spammers and phishers by making them work much harder to overcome preventative safeguards.

Given the complexity of effecting change in the global email infrastructure, there are many benefits to having multiple authentication techniques. IP- and signature-based solutions used in concert will result in more robust solutions that can work with an array of platforms, user environments and deployment requirements worldwide.

## Filtering Technologies

Filtering technology remains a key component to stopping spam, and technology companies must continue to invest heavily in research and development of filters that more effectively distinguish between legitimate email and junk messages. Microsoft's SmartScreen™ technology, which uses probability-based algorithms to assess the likelihood that a message is spam, has achieved excellent results. The company also is preparing to deploy anti-phishing technology in its email and browser products to further reduce consumers' exposure to fraudulent messages.

## Prevention Technologies

Technology companies are working together to create interconnected and "smart" agents that can help derail outbound spam at the ISP level. Additional prevention efforts include providing anti-spam tools and best practices that can help ISPs more swiftly recognize new spam, phishing and email-borne virus attacks.

## Industry Collaboration

Spam and phishing are problems that strike at the heart of all technology companies and thus demand industry-wide cooperation that transcends competitive interests. Organizations such as the Anti-Spam Technology Alliance (ASTA), Anti-Phishing Working Group (APWG), Global Infrastructure Alliance for Internet Safety (GIAIS), and the Coalition on Online Identity Theft are just a few examples of industry-wide teamwork under way to counteract spam, phishing and other email threats. Also, as detailed in the preceding section, leading technology companies – many of them traditional competitors – are collaborating on technology approaches. Various industry leaders also are working closely and effectively with governments on public policy and cooperative enforcement efforts.

This deep cooperation across industries, interests, and borders is essential to advance the objective of shutting down spam and phishing businesses worldwide.

## End-User Education and Enablement

Consumers' growing frustration with spam and other forms of deceptive messages online is leading many to curtail or even abandon their use of email. In order to restore confidence in this important medium, end-users need to know more about the risks they face online and how to limit their exposure.

Promoting greater awareness of new and evolving threats is one of the most direct lines of defense against the advance of spam and phishing. Microsoft and others provide a host of educational tools and resources, ranging from step-by-step instructions for activating anti-spam tools on the PC to reporting spam and phishing incidents, at these and other Web sites:

- Federal Trade Commission (FTC) Spam for Consumers page – <http://www.ftc.gov/bcp/conline/edcams/spam/consumer.htm>
- APWG Web site – <http://www.antiphishing.org/>
- Internet Fraud Complaint Center Web site – <http://www.ifccfbi.gov/>

- MSN Online Safety & Security – <http://safety.msn.com/>
- Microsoft Security at Home – <http://www.microsoft.com/athome/security/default.mspx>
- Microsoft Trustworthy Computing: Spam – <http://www.microsoft.com/mscorp/twc/privacy/spam.mspx>
- Microsoft Trustworthy Computing: Security – <http://www.microsoft.com/security/default.mspx>.

## Legislation

Increased legislative activity aimed at thwarting spammers and phishers, both in the United States and internationally, is vital to helping make these activities less attractive and lucrative to perpetrators. The recently enacted US CAN-SPAM Act, with its strong enforcement provisions for ISPs and state attorneys general and its criminalization of deceptive spamming techniques, has already proved highly valuable in taking the fight directly to the largest and most brazen spammers. Because spam operations are so easily and inexpensively transported from one location to the next, it is also vital that technology industry leaders continue to step forward to assist governments around the world in passing similar legislation and creating effective enforcement models.

Although laws may vary country by country, there are common themes to effective anti-spam legislation anywhere in the world, including provisions that support the following outcomes:

- Dramatically reduced volumes of spam;
- Greater consumer control over whether and how to receive, filter and delete messages;
- Incentives and support for legitimate marketers who seek to use email responsibly;
- Preservation of existing tools employed by ISPs to fight spam; and
- Prohibition of falsified name or transmission information to hide the identity of the true sender, and of using methods to circumvent consumer or ISP-implemented spam-fighting technologies.

Policymakers should continue to reach out both to industry stakeholders and to each other to find common ground and strive for consistency in anti-spam policy worldwide.

## Enforcement

As with the industry collaboration efforts detailed above, Microsoft welcomes opportunities to assist government agencies at the state, federal, and international levels in assuring that perpetrators of illegal spam meet with strong consequences. Robust enforcement of anti-spamming and anti-fraud laws is essential to stripping away the financial rewards as well as the cloak of anonymity that spammers and phishers have enjoyed.

The CAN-SPAM Act provides a national, uniform standard for filing lawsuits against spammers and criminalizes specific spamming techniques, empowering state attorneys general and the Federal Trade Commission (FTC) to crack down on illegal spam operations that violate CAN-SPAM provisions. Microsoft directly supported the FTC's first criminal enforcement action against spammers under CAN-SPAM in April 2004 and applauds continuing work by government enforcers.

CAN-SPAM also enables technology and Internet service providers to more effectively pursue civil lawsuits against suspected spammers. For example, America Online, EarthLink, Microsoft and Yahoo! joined together to file the first major industry lawsuits under CAN-SPAM in March 2004 and a second series of suits in October 2004. Also, Microsoft partnered with Amazon.com in September 2004 to file lawsuits against spammers and phishers in the United States and Canada.

Various state laws provide additional avenues of pursuit against cybercriminals. In September 2004, Microsoft filed a lawsuit under the state of Washington's strict anti-spam law against a so-called "bulletproof host," which was providing web-hosting services to bulk emailers. Microsoft supported a state lawsuit and filed a coordinated action with the state of New York in December 2003 against a top spamming ring; the company also participated in a similar filing action with the state of Washington in June 2003. In sum, Microsoft has to date filed more than 75 lawsuits in the United States against spammers and has been awarded more than $79 million in judgments as of August 2004.

While international efforts to sanction spammers and phishers have been somewhat hampered by inconsis-

tent – or non-existent – laws from country to country, technology companies' continued dedication to sharing expertise and resources with government agencies is invaluable as they seek to build stronger anti-spam frameworks. In the United States as well as abroad, creating long-term partnerships with law enforcement agencies and prosecutors in the area of Internet safety is among Microsoft's top priorities. This has included providing direct support behind more than 100 worldwide legal actions against spammers by governments in countries throughout Europe, Asia and South America.

## The Road Ahead

While a solution that thoroughly eliminates the scourge of deceptive and unwanted email remains elusive, there is reason to be optimistic about the collaborative progress being made by industry, government and consumers toward curtailing the volume and malicious effects of spam. These collective efforts also are helping to enhance the reliability, efficiency and safety of computing in general. Microsoft is committed to working at the front lines of this campaign until spam ceases to be a significant concern for the global community of Internet users.

# Spam, Economics and Democracy

*Phillip Raymond, CEO*
*Vanquish Inc.*
*http://www.vanquish.com*

Common anti-spam techniques, at best, put a temporary band-aid on a festering sore. More typically, they throw out the baby (freedom to engage a receptive audience) with the bathwater (spam). This paper describes an approach that thwarts the economic engine that facilitates spam, while still allowing free and open communication.

This presentation defines the problem, briefly shows why existing anti-spam measures are ineffective, and describes a system based on economic principles that will ultimately solve the problem in a manner acceptable to all parties: commercial enterprises, officials and individual users – including those who expect a right to privacy and freedom from interruptive communications.

## The Rise of Email: Faster Than the Telephone

Email emerged from its academic roots only fifteen years ago. In this short time, it has surpassed the telephone and the post office as the world's most popular communications medium.[1] The speed at which users adopted email seems unlikely. The telephone, for example, has had a 125-year head start. It supports two-way conversation (including interruption and immediate clarification) and the impact of emotion. It also requires less expensive user equipment and fewer skills.

Rapid adoption of email can be attributed to four benefits, each a hallmark of the Internet in general. Email is free, fast, simple and democratic. Spam is a side effect of nearly free transmission and the power of computers to replicate content, regardless of its relevance to individually addressed recipients.

1. Worldwide Email Server Software Markets. Frost and Sullivan. March 1, 1999.

## How Is Email "Democratic"?

Email is the only medium in which anyone can initiate contact with anyone else, without cost, complexity, or concern for geography, time zones and obstacles erected by governments and communities. But free and universal access between strangers brings a deluge of irrelevant contact. Recipients can erect filters against the onslaught of spam, but the ideal solution requires no effort by either party, and blocks only messages that would irritate a recipient, if he were to know the content.

## Existing Practice: Intuitive Approaches Are Ineffective

Existing anti-spam methods interfere with one or more of email's benefits – that it is free, fast, simple and democratic.

Spam fighting techniques run the gamut, but can be divided into six well-defined categories: lists, filters, challenges, legislation, sender identification, and payment mechanisms.

| Mechanism | Ef | Fr | Fa | Si | De |
|---|---|---|---|---|---|
| Personal Lists | P | ✔ | ✔ | ✘ | ✔ |
| Community Lists | ✘ | ✘ | ✔ | ✔ | ✘ |
| Filters (heuristics) | ✘ | ✔ | ✔ | ✔ | ✘ |
| Challenge-Response | P | ✔ | ✘ | ✘ | ✘ |
| Legislation/Bounties | ✘ | ✔ | ✔ | ✔ | ✘ |
| Sender ID | ✘ | ✔ | ✔ | ✘ | ✘ |
| Payment Mechanisms | P | ✘ | ✘ | ✘ | ✘ |
| Sender Risk ('Bonds') | ✔ | ✔ | ✔ | ✔ | ✔ |

Table 1 – Most anti-spam techniques interfere with one or more of the principal benefits that made email popular.
Ef = Effective
Fr = Free
Fa = Fast
Si = Simple
De = Democratic
P = Partially Effective

Current anti-spam products and services use a combination of these methods along with a personal list of allowed and blocked senders. They attempt to combine advantages of each method while avoiding the interception of desirable mail.[2]

- Lists and filters try to identify characteristics that are often associated with legitimate mail. Even if they could do so accurately, they apply community censorship to personal mail.
- Challenge-response delays legitimate mail and purchase receipts, search agents, newsletters and shipment data.
- Legislation and bounties are like prohibition. The economic incentives of spam render the legal deterrent ineffective.[3]
- Sender identification requires a massive international registry to be effective. It punishes new domains and email addresses and makes senders accountable for past behavior of providers or other domains using the provider. It unnecessarily strips anonymity, yet it has no bearing on the relevance or urgency of a message. Even if widely adopted, sender ID schemes will fail to stem the onslaught of spam.
- Payment schemes conflict with free access and the origins of the Internet as champion of a level playing field. Of course, recipients have a right to restrict access, but even if fees could be levied only upon senders of unsolicited commercial mail, a preferable method allows unfettered contact by unrecognized senders who can tangibly demonstrate that their message would be desired by each addressed recipient. Such a system can be easily implemented by placing the sender at financial risk.

Filters and lists are defensive in nature. That is, they provide a mechanism for blocking mail based on "negative" criteria rather than guaranteeing delivery based on positive criteria. Therein lies a problem. When used in combination, the individual advantages of each approach are not additive. In fact, the disadvantages multiply. Additionally, the techniques interfere with one or more of the principal benefits of email.

Challenge-response, identification, and payment mechanisms attempt to legitimize a message or its source rather than block it, but they address the wrong problems.

## Spam: A Universal Definition

To thwart spam, we must first agree on a definition, and then determine what facilitates abusive behavior on the part of spammers. Few people agree on a definition. Most people associate spam with mail that is unsolicited, commercial or sent in bulk. Yet they acknowledge that desirable mail often has one or more of these characteristics. The real bane of email is not that a message is commercial or sent by a stranger, or even that it was sent by someone without a verifiable reputation. A much more basic definition can lead to an effective method of dealing with it:

> *Spam is any message that you wish you had not received.*

Spam, then, could be any message that is irritating, harassing or simply irrelevant. But in any case, it is characterized by the fact that an individual recipient personally found it to be personally objectionable. This simple definition leads to a very simple logical construct:

- Spam is undesirable mail.
- Undesirable mail is a product of poor targeting.
- Poor targeting is encouraged by economic incentives.
- Solution: Create an economic disincentive.

## Conflicting Goals: Simplicity and Customization

There is a growing awareness among all sectors – government, email providers and users – that an effective solution to spam must contain a strong economic deterrent. But simply crafting an economic solution will not ensure its adoption. Widespread adoption of an economic spam deterrent requires that it also be practical. Like email itself, a mass-market

---

2. An expanded comparison of anti-spam technologies is available at <http://www.vanquish.com/whitepaper/>.

3. Legislation can be evaded by jurisdiction, the cost and complexity of tracking, and the ease of demonstrating a plausible relationship. The prospect of draconian penalties is more likely to suppress mailings by the most legitimate and desirable commercial senders.

mechanism to stop spam must be affordable and demand little or no configuration and user training.

In addition to being inexpensive and simple, a spam solution must effect a deeply personal decision–the extraction of desirable contact from that which is irrelevant. You may not be searching for a discount hotel in the Caribbean this week, but someone else is. Even a very popular spam topic, like Viagra, must be discussed between doctors and their patients. Effective anti-spam must be tailored to the individual needs of recipients without requiring training and without compromising the privacy of its users.

Simplicity and end-user customization: Two conflicting goals must be satisfied to make a solution practical.

## Correcting Behavior: Make Senders Responsible

Proponents of sender identification claim that spam will dry up if senders are identified or at least forced to use genuine and traceable email addresses. The phone company uses such a "Caller ID" method today. They routinely intercept messages that lack Caller ID for recipients who choose to screen calls. But the phone number of an unrecognized caller says nothing about the relevance and timeliness of the message content to the needs of the recipient. The call could be from a relative in a hospital or from a marketer with no better demographic data then a phone book. The only reason we are not swamped by thousands of untargeted phone calls each day is because of the cost and effort associated with each call.[4]

Suppose, instead, the intercept message said this:

> *"Your Caller ID is not recognized by the party you have dialed. If you complete the call and the recipient finds your contact undesirable, they may press *77. This will add a $2 fee to your phone bill."*

In the above scenario, *77 is an "interrupt penalty." In effect, it says "I found your message to be irritating, harassing or irrelevant, and so I will prod you to either refine your address list or deliver better content." In a two year trial of this type of voluntary sender liability applied to email, recipients rarely use their power to penalize senders. Instead, filtering occurs in the mind (and the pocketbook) of the sender.

Spammers send their drudge to audiences that are both large and poorly targeted. But they abandon those recipients who demand such a bargain. A properly implemented system ensures that known addresses are exempted from the process and that methods for senders to put up money are trivial and trusted. Such a design facilitates adoption.

Most importantly, the "sender-at-risk" model facilitates commerce. It allows marketers to reach prospective clients if they are willing to back their unsolicited contact with a warranty of individual relevance.

## Economics 101: Correcting the Imbalance

The successful solution admits messages based not on content, but on the *value of the content to the individual recipient, and the tangible cost associated with interrupting him*. The construct of such a system would seem a fantasy, especially when you consider that it must be automated, personalized, accurate, self-adjusting, transparent and virtually without cost.

A sender-at-risk solution to spam that meets these criteria is gaining momentum. It is backed by cryptographic authentication, but unlike other identification schemes, digital signatures identify the cash at risk, and not necessarily the sender or service provider. It leaves desirable email free while making the irritation of strangers too costly for senders who are not certain that their mail is invited – or otherwise welcome.

While not obvious, such a system can be built without complexity. It embodies the same economic principles that deter spam in every other medium used for commerce, but without imposing a cost on email, which can remain free. The method represents much more than a perfect solution to spam. Rather than just retard poorly targeted commerce, it invites desirable contact – when and how a recipient desires it.

It can transform email, phone, fax and text messaging into tools that attract personally desirable information. *Information that you want*. Not just from friends and pre-subscribed sources, but from all sources that can demonstrate confidence in the appropriateness of their message for each addressed recipient. Just as individuals look forward to receiving their favorite trade magazine, email can be an anticipated pleasure. With the power and ubiquitous nature of the Internet,

4. Ayres, Ian & Nalebuff, Barry. Want to Call Me? Pay Me! *Wall Street Journal*, Oct 8, 2003

the content will not be all about gardening or model airplanes; it will be *all about you*.

Magazines and television are inherently expensive. Email and other forms of electronic messaging are inexpensive. Content can not only be tailored, the delivery of that content needn't be costly to either party – not to the sender in dollar and cents and not to the recipient in time lost to unwelcome interruption.

Privacy advocates at Vanquish Inc. have demonstrated a service and an appliance that satisfy these criteria simply and effectively. Readers of this compendium can put it to work on their personal email address immediately.[5] It preserves all aspects of a free and open communications network while guaranteeing that recipients will be satisfied with each message, even those from strangers. The Vanquish approach:

- preserves sender privacy (the recipient's ability to seize cash is confirmed, but not the sender's identity);
- does not require widespread adoption to be effective;
- results in a satisfied recipient – or a recipient who has been compensated for his inconvenience;
- does not require replacing SMTP or other standards; and
- preserves the benefits of email. It remains simple, inexpensive, instantaneous, and democratic for senders – but not for spammers.

## Three Economic Approaches: Risk Beats Payment

Three vendors are at the forefront of the search for an economic solution to spam. Each offers a different approach.

### Company "G"

"G" is preparing to introduce "E-postage." Senders pay a flat fee when mailing to users of participating email services, if the addressed recipient has not previously waived payment for that sender. The model has two significant design flaws:

- The fee is paid to a third party rather than the recipient.
- The fee is paid even if the recipient enjoys the message.

Even if a recipient could levy fees only on senders with a marketing agenda (an impossible distinction and one that shouldn't be made), it would impose a cost on a medium that does not embody an inherently costly mechanism. This punishes unrecognized senders, and mail that is commercial, automated or sent in bulk – even if the content is perfectly acceptable to the recipient. This chilling impact on free access can be avoided by a system that permits recipients to instantly and irrefutably penalize any unwelcome message. The result is not a system of penalties but rather a system of deterrence.

### Company "I"

"I" offers a program of sender bonding designed to convey legitimacy upon senders of bulk mail (customers who purchase their commercial mail servers). With the bond as a badge, "I" lobbies ISPs and mail providers to waive their client's mail past filters, because the sender is at risk. If "I" receives a high number of complaints, money deposited by the sender is paid to a charity or other third party.

As with filters, this filter-bypass system empowers third parties, not recipients, to determine what flows into inboxes. Recipients have little say in what they receive, except to complain.[6] More importantly, collected funds are not the property of the irritated recipient. Inherent in the "I" definition is the assumption that desirable contact can be gauged by impersonal collective complaints or statistical metrics. Finally, the developers have tied the mechanism to a trust registry. In an ideal system, however, the past behavior of all parties is irrelevant. What matters is the earnest money that a sender is willing to risk. It is the only certain demonstration that he or she has researched and respects the individual preferences of each targeted recipient in a given mailing.

A better implementation would not collect postage unless a recipient deems a message irritating or irrelevant. That decision would automatically set the risk

5. <http://www.vqme.com> Readers may experiment with up to 5 email addresses without charge. Access clean email from any PC, even without software.

6. Wetzel Rebecca. Spam Fighting Business Models — Who Wins, Who Loses, *Business Communications Review*, Apr. 2004.

requirement for other senders. Most importantly, if a recipient seizes the money, it is his to keep.

### Company "V"

For the past two years, Vanquish Inc. of Marlborough MA has been testing an email warrant system that empowers recipients to collect cash from unrecognized senders instantly and effortlessly. Individuals from 16 countries and 100 ISPs tested incoming mail for bonds and additionally bonded outbound mail. More than 3 million messages were passed between senders who incorporated the bond and recipients who were empowered to recognize and seize payments. A feedback mechanism allowed senders to avoid sending to recipients who penalize a high percentage of sender bonds. Despite an audience that was skewed toward the most ardent advocates of privacy, no penalties were issued throughout the test.[7]

## Interrupt Value: Senders Bid for Your Attention

There is little doubt that a small, but fixed, cash risk associated with each message would shut down the most egregious spammers. But in practice, it would only change the nature of the spam and not the quantity. Economic models demonstrate that solicitations for higher value services would backfill the channel with equally untargeted pitches and in the same quantities.[8] Recipients would be afraid to raise their cash-risk barrier, because it would dissuade desirable contact.

An ideal system must not only accommodate different cash-risk demands for every user – it must also adjust dynamically to the needs of each user and how valuable their time is from day to day. Finally, it must do so without demanding that the protected recipient guess the monetary value of their attention.

How high a barrier should one erect against unsolicited contact? A barrier set too high discourages relevant and interesting mail. Set the barrier too low, and marketers have no incentive to refine their mailing list. Fortunately, email recipients needn't guess at the value of incoming communications. Implemented correctly, an economic system pushes the work back to the sender. In effect, feedback mechanisms play a much bigger role than preventing unfair seizure. They take the guesswork out of placing a monetary value on time.

A *bid-for-attention* feedback mechanism creates an effective process in which the "interrupt value" of each protected recipient is automatically adjusted based on the number and confidence of unrecognized senders who seek to reach him. The recipient specifies a number of permissible interruptions (typically, the number of desirable messages that were incorrectly intercepted by classic filters). This threshold for unsolicited contact, along with his popularity as a target, is translated into the instantaneous value of his time. This, in turn, factors into the behavior of senders. Those with the most confidence in their ability to escape the recipient's wrath do not fear the process. But senders without intimate knowledge of a recipient demanding such a cash guarantee of relevance would never attach the risk to their message.

Of course, this mechanism raises the question of how much interruption to allow. Setting this "interrupt value" is much easier than experimenting with monetary values because it is equal to the number of desirable messages your legacy spam filters had blocked in a typical day. Set the interrupt allowance too high and poorly targeted messages get through. Lower it, and continue to receive the unsolicited messages that are interesting and relevant. Most email users are surprised to find that the right value never discourages relevant contact, and yet consistently blocks messages that they would personally find undesirable.

A sender risk mechanism with a feedback system and a bidding process may sound complex, but it can be transparent to both senders and recipients. These processes are already at the heart of every other communications medium. They result in a dynamic mechanism that converts the intangible value of interrupting each individual recipient into cash risk. It is the only solution that guarantees free speech while making irrelevant contact unprofitable. For protected recipients, only two outcomes are possible: they will personally desire receiving their mail or they will be wealthy. Wealth is a unlikely outcome, because the decision to send desirable mail is made by the sender based on his or her confidence in knowing the interests of the recipient.

## Stretching the Bond

How much money must be at risk by a typical sender to signal gateways at the recipient mail provider that

7. BETA-1 AND BETA-2 Vanquish Pro (software) and vqME (a web service). January 2003~January 2005.

8. Van Alstyne, Marshall et al. Information Asymmetry and Thwarting Spam, University of Michigan, 2004.

the message is not spam? Surprisingly little! A $2 bond may be sufficient indefinitely. The amount is small enough that it could be bundled with a package of other services, making it unnecessary to even ask users to put money at risk. With such a small amount at stake, the system would appear to be open for abuse. But together, several design factors make a small bond extremely powerful while still making it prohibitively expensive for participants to send spam.

Senders are liable only to recipients who are newly contacted, able to detect a bond, and only for 72 hours. At present, the default risk associated with unsolicited email is US 5¢, an amount that has been sufficient to stop spam while still being low enough to avoid frightening friends and desirable commercial senders. A $2 bond covers the liability associated with 40 messages. But the nickel is only frozen for messages that meet three conditions: the message was sent to a stranger, the stranger can test for its presence, and the message was sent within the past 72 hours. Ultimately, the only senders who must add to their bond are either bulk mailers or individual senders who frequently irritate addressed recipients. That is, the bulk mailer increases his available bond to cover a large mailing to new customer prospects while the penalized individual sender replenishes his bond to replace money seized by recipients.

How is it that a sender is liable only for messages sent to strangers? If the person targeted by a sender has previously sent mail to that sender or engaged in a web site transaction, the token embedded by the sender is converted from a cash bond into a "Trust Bond" – a digital signature that proves a message is from a previously trusted sender. It needn't reflect cash at risk unless a recipient revokes the trust, and it doesn't even identify the sender. Instead, it offers digital evidence of the parties' past communications and the fact that the recipient did not previously choose to penalize the sender. As adoption spreads, senders grow their list of "Trust Bonded" recipients. In effect, recipients individually waive the right to penalize trusted senders "until further notice."

A Trust Bond does not necessarily identify the sender. Instead, it is digital evidence of personally acceptable conduct.

## Beyond Anti-Spam: Funding the Infrastructure

So far, we have addressed spam only as a drain on the resources of email recipients. However, there are two other parties to the transaction who suffer at enormous cost: legitimate business senders whose bulk and automated mail is intercepted and ISPs who deal with the bandwidth and the customer dissatisfaction of both spam and of incoming mail lost to spam filters.

Every communications medium is a vehicle for commerce: magazines, newspapers, television and phone. With the exception of email, advertisers pay for distribution of both their commercial message and editorial or entertainment content. Often, subscriber fees don't even cover the distribution cost.

A ¼ page ad in the Sunday New York Times costs $30,000.[9] Advertisers don't expect free access to subscribers. The high barrier to entry forces commercial senders to carefully consider readership demographics and the placement of their message into the appropriate section. The cost also assures an engaged reader but keeping the channel free of chafe. This same economic friction sets apart CBS from CB radio.

But unlike these other communications media, email presents no barriers to the sender—even when a message is delivered to a million recipients. No actors, no production, no postage, no fuss. Not even an incentive to research market demographics or demonstrate concern for the burden placed on the rest of the channel. Why bother? It's practically free. One response in a hundred thousand generates a profit. But free access for all comers creates a very costly problem for the legitimate commercial sender - the ones that demonstrate respect for the time and resources of each addressed recipient.

Despite its wealth of instant information, the Internet lacks the friction of sender payment. As a result, ISPs – the independent delivery agents – are near bankruptcy and users are inundated with irrelevant contact. The sender-pays model has two effects: the sender has an incentive to target messages appropriately and the channel is funded by the senders who generate the traffic. Recipients are well informed and happy.

A refinement of the Vanquish model allows a sender to embed a small payment to the recipient ISP as an incentive to inspect arriving mail for a bond. This fee, say ½¢, is not sufficient to assure the ISP that

9. 2004 Advertising Rate Card, *New York Times*, <http://www.nytadvertising.com/was/files/others/2004_Rate_Book_PDF_Auto.pdf>. Cost depends on regional/national editions, number of insertions, and the use of optional color.

the message is suited to each targeted recipient. But the larger cash bond (also embedded in the message) offers such a guarantee. The result: the sender has engaged the recipient with a clean channel; the ISP funds the build out of his distribution channel – just like any publisher; and the customer receives only relevant contact. From a marketing standpoint, the cost of acquisition is far lower than any other medium and with an ability to better measure response and refine both content and targeting.

The optional mechanism of a small cash payment by senders – only for the portion of their mailing list that is newly contacted recipients – also creates a natural adoption vehicle for this novel approach. As long as the bulk sender can identify a few ISPs that have blocked large numbers of messages in the past, this arrangement of pay-for-bond inspection does not require a critical mass outside of the agreement.

## Conclusion

A truly democratic email system allows each individual to pursue his or her interests while remaining accessible to those with similar interests. The problem with Viagra, mortgages and even pornography is not that people sometimes search for these things on the Internet. *The problem is that these things are searching for you*. A lack of economic incentives makes your email address fair game.

The most important benefit conveyed by a properly designed system of sender liability is that it enhances the value of an email address over time. With all other anti-spam methods, an email address loses its value over time—as it is harvested by spammers. Eventually, users retire addresses or create separate addresses for commerce, newsgroups or other public venues. Gradually, they have less and less time to check for mail at these unguarded addresses, because so much of it is irrelevant. When unrecognized senders are held accountable, there is no need to hide an email address. Instead, *the more it is disseminated, the more personally relevant and interesting content it attracts* – especially from strangers who are willing to demonstrate such high confidence in the individuals they target.

Vanquish has crafted a pure economic solution that leaves email free, fast, simple and democratic. Only spammers will fear the mechanism of voluntary financial liability. Careful commercial senders recognize the value of a clean channel in which they can engage willing recipients only.

# Spam Fighting: Authentication, Accreditation and Reputation

*Des Cahill, CEO*
*Habeas Inc.*
*http://www.habeas.com*
*des -at- habeas.com*

## The Problem

A direct consequence of the proliferation of spam (and the spam-filtering industry that has sprung up to fight it) is that email has become an increasingly unreliable method of communication. The cost to businesses of fighting spam has become enormous. Radicati Group, a market-research firm, estimates that corporations will spend $635 million on anti-spam products and services in 2004. One of the biggest issues businesses face is that the same technology they've purchased to thwart spam is also frequently preventing legitimate messages such as transaction confirmations and financial statements from reaching their intended recipient — a source of major customer dissatisfaction. And the problem is getting worse.

The many spam-related problems faced by legitimate volume senders of email and individuals who depend on email to conduct business have turned an otherwise inexpensive and convenient means of communication into a source of costs and frustration. Consider just some of the many negative effects that spam has created for all users of email:

- According to the Pew Internet & American Life Project, a non-profit organization that studies the Internet's effects on society, 63% of email users say spam has made them less trusting of email in general. Additionally, 73% of email users now give out their email addresses less often than before, and 69% avoid posting their email addresses on the web, for fear of spam.
- The Radicati Group, a market-research firm, estimates that corporations will spend $635 million on anti-spam products and services in 2004.
- In a 2004 report ("Overcoming the Spam Effect"), analyst firm Jupiter Research forecasts that the cost of blocked emails alone will jump from $230 million in 2003 to $419 million in 2008. The report also notes this forecast is conservative, because it does not factor in the added opportunity costs of emails that would have resulted in business transactions.
- According to analyst firm Nucleus Research, dealing with spam costs $874 per year for every worker with email. With roughly 100 million such workers in the United States, the total cost for this problem is over $87 billion annually.

Clearly, spam is far worse than a mere annoyance. It is wreaking havoc on the entire email system – costing billions of dollars, draining untold amounts of productivity and eroding the trust on which we all depend for email to remain a viable communication tool for business and personal use. In response to the problem, ISPs and other major email infrastructure players are collaborating to find ways to out-smart spammers.

## Authentication Is Just the Start

*Authentication standards* from Yahoo!, Microsoft and other major players enable receivers to believe that senders are who they claim to be. Progress has been good in this area. It's looking more and more likely that receivers will be able to converge on a set of standards that will enable them to determine whether the sender is really who he claims to be. That won't be sufficient but, nonetheless, the move toward Sender-ID standards is a positive and necessary step.

Criminals are an ingenious bunch and the determined spammer will figure out how to procure a "good identity." These identity-focused approaches marry the "From" address and IP address/domain. Unfortunately, this approach doesn't tell us whether the email is:

- spam; or
- from a legitimate company, but undesirable email nonetheless; or
- from a legitimate company and "wanted" email.

Another encouraging development is AOL's move toward providing sender feedback in its spam-filtering processes. Such practices are helping legitimate senders understand how their messages are being perceived and rated by AOL's subscribers – a first step toward helping senders improve their practices.

What's still needed is a way to ensure that legitimate senders of volume email have a way to signal to receivers who they are, and to declare their email as "good." That's where email accreditation come in.

## Accreditation – The Next Step

Accreditation services build upon the foundation provided by identity authentication standards, providing certification that an email sender complies with recognized best practices when sending email. This is a crucial addition to sender-side solutions. These accreditation services, combined with identity standards, can enable true identification of legitimate email and reliable delivery of an email to its final destination.

To earn accreditation, a legitimate volume email sender undergoes a rigorous process that guides the company through the implementation of best practices in sending email, ensures it complies with email laws, and earns it a reputation as a trustworthy sender.

Accreditation involves an objective third-party expert submitting the sender to a six-step process that transforms it to a *bona fide* whitehat (i.e., known good) emailer, as follows:

1. *Certification* - The first step in transforming a company into a whitehat sender includes a thorough audit of its current and historic email practices and an assessment of its reputation. This process involves interviewing people throughout the company to determine the types of email they send, how quickly they respond to complaints, and other crucial issues about their email sending practices. The process also includes researching exactly how the company is perceived as a sender—its corporate "email reputation"—by searching the Internet for negative messages, determining if the company is on blacklists and learning how it is regarded by ISPs.

2. *Classification* - The next step involves classifying the company's various mail streams. Examples include "single opt-in" emails, in which a user simply signs up once, or stricter "confirmed opt-ins," where a user signs up, then receives an email requiring a click on a link to confirm the transaction. When the third-party accreditation expert understands the different types of mail streams the company sends out, it is better positioned to help it improve its practices.

3. *Compliance Monitoring* - In its transformation to whitehat sender status, the sender submits to an ongoing process to ensure it complies with all laws and continually adheres to the highest standards of ISPs. (In the age of CAN-SPAM and other emerging anti-spam laws, compliance monitoring is no longer a luxury – it is a necessity.) A good compliance process also includes a feedback mechanism allowing recipients to register complaints about bad practices.

4. *Tracking* - Because email senders have historically been blocked from receiving feedback about the percentage of their email that reaches recipients' inboxes and the percentage diverted to spam folders, the third-party expert compiles and monitors this information and provides it to the volume sender so it can quickly modify its practices in order to avoid damaging its email-sending reputation.

5. *Delivery* - After a sender has undergone these steps, and as a result has improved its email practices, the third-party expert can vouch for the company's email with volume receivers as being safe and legitimate – ensuring the company's mail is delivered.

6. *Mediation* - In this final step of the sender's conversion to whitehat status, the third-party expert serves as a mediator on the company's behalf in any disputes with ISPs or other volume receivers. Of course, because the company would have adopted stringent and responsible email-sending practices, such disputes would be extremely rare.

## Reputation – The Missing Link in Sender Identity

Today's receivers (i.e. ISPs) are faced with the enormous costs of filtering spam, but at the same time they are concerned about falsely classifying a legitimate email as spam, since doing so results in dissatisfaction on the part of their customers. What if there were a way for receivers to discern the email

"habits" of the sender of email entering their system? And how about a way for consumers to let receivers know which email is really spam?

As a company focused on accreditation and reputation, Habeas is actively enabling these key elements of a healthy email ecosystem.

Once accreditation and mediation standards are in place, it becomes easier to gather reputation data on accredited senders and make that information available to volume receivers such as ISPs, web-mail providers, anti-spam providers, enterprises and small to medium-sized business. Armed with the knowledge of who the sender is and the type of email that person or organization sends, it's now possible to build a "reputation profile" of the sender. Habeas can then publish this information and make it available to receivers as a reliable basis for assessing future emails from that sender.

This is great news for *receivers* since it enables them to deliver legitimate email and focus their anti-spam resources on determining whether the remaining email is legitimate or spam.

Legitimate volume *senders* also benefit since their good reputation will enable them to reliably reach their customers and reinforce their relationship with that customer. Consequently, email is restored to its role as a convenient means of staying in touch with customers, and senders have a good reason to stay on the "right side of the law."

But, most of all, it is *consumers* who stand to gain the most from these advances. The combination of authentication, accreditation and reputation will mean that consumers will receive much less spam, and will be able to report spammers to receivers with an assurance that their vote will be factored into the way that future email from that sender is handled by receivers.

## About Habeas

The proliferation of spam, and the response to it, has made email an unreliable medium for legitimate business communications and ecommerce. Habeas is helping to build a sustainable model for email so that legitimate businesses can consistently use email to communicate with their customers, and so that ISPs can be confident that email from these businesses consists of legitimate business-critical communications. Habeas' solutions enable companies to comply with the latest standards and regulations; to identify themselves as adopters of email best practices; to outsource the monitoring and resolution of their email delivery problems to experts at Habeas; and to track and increase the delivery rates of their legitimate email.

# Identifying Legitimate Email: The Email Accreditation Services of TRUSTe

*Fran Maier, Executive Director & CEO, TRUSTe*
*fmaier -at- truste.org*

*Colin O'Malley, Director of Product Development, TRUSTe*
*colin -at- truste.org*

Three years ago, TRUSTe[1] identified spam as one of the most important threats to trust in the networked world. TRUSTe has played a leading a role in the proliferation of privacy statements on the Internet since its founding in 1997, creating higher expectations for consumer notice and standards for appropriate use of personal information. All of TRUSTe's programs feature program requirements that balance a complex mix of legislated standards, industry reality, and consumer expectations. Through our relationship with the Bonded Sender Program, the leading legitimate sender program on the market, TRUSTe has been able bring the benefits of its process to the email community to combat spam. This article will focus on key lessons learned from the Bonded Sender Program and further efforts by TRUSTe to elevate the role of consumer concerns in the war against spam, including a new consumer trust mark and an emerging accreditation policy framework.

## The Initial Approach: Bonded Sender Program

TRUSTe's primary effort as an Independent Trust Authority for email has been serving as the accreditation and enforcement authority behind IronPort's Bonded Sender Program (BSP). With the successful introduction of the Bonded Sender Program, TRUSTe is now the gold standard of email accreditation authorities. The Bonded Sender Program, for which TRUSTe provides certification, oversight and dispute resolution services, brings accountability to email with a unique complaint rate enforcement mechanism. TRUSTe certifies participating senders to a baseline set of standards that include consent with robust disclosure and easy unsubscribe tools, as well as technical requirements to ensure that mailers' servers do not assist spammers. Senders must post a significant bond that is debited in the event that consumer complaint rates surpass set thresholds. ISPs participating in Bonded Sender's network agree to deliver email from Bonder Senders, producing increased delivery rates for senders who can maintain low complaint rates.

The Bonded Sender Program was the first of a class of legitimate sender programs and has achieved significant success in its first year of operation, amassing over 35,000 receiving networks and more than 130 email senders, including Hallmark, CNET, Match.com, Intuit, About.com, and MSN. Developing the Bonded Sender Program required a comprehensive understanding of the dynamics of the current ecosystem and deep knowledge of the full range of existing and emerging technologies aimed at reducing spam.

## How Bonded Sender Works

Before the creation of legitimate sender programs, spam solutions focused primarily on protecting receiving networks from bad mail. The traditional solutions included "black lists" of the worst senders on the Internet and spam filtering products that scanned each incoming message for characteristics associated with bad email. These solutions have played important roles, but they have also produced unintended consequences. In particular, email senders that recognize the critical importance of consumer privacy regularly find their messages mistakenly identified as bad email by anti-spam solutions. When this happens, messages are blocked from reaching their intended recipients, often in a manner that is invisible or unclear to the sender, reducing the reliability of email as a communication medium and representing a considerable threat to the cost efficiencies email brings to the global economy. Such filtering errors are called "false positives" within the industry. In recent

1. TRUSTe is an independent, non-profit organization dedicated to enabling individuals and organizations to establish trusting relationships based on respect for personal identity and information in the evolving networked world. Founded in 1997, TRUSTe runs an award-winning global privacy certification and seal program. Its seal programs are considered Safe Harbors for the Children's Online Privacy Protection Act (COPPA) and the EU Safe Harbor Framework. Today, TRUSTe maintains the largest privacy seal program with more than 1,400 Web sites certified throughout the world including AOL, Microsoft, IBM, Nationwide and The New York Times. TRUSTe's mission extends standards, certification and oversight into email with Bonded Sender and into wireless with the Wireless Advisory Committee. For more information on TRUSTe visit <http://www.truste.org>.

years the false positive problem for email filtering has reached dramatic levels, with many studies estimating that 15% of legitimate email never reaches the inbox. At its core, the Bonded Sender Program is a service designed to solve the false positive problem for senders of legitimate email.

By joining the Bonded Sender Program, senders of email improve their delivery rates. In a recent analysis of the program's effectiveness, CNET found that participating in the Bonded Sender Program reliably lifted open rates, their best proxy for delivery rate, by 15%. CNET came to this conclusion after running a series of 63 test campaigns involving 300 million messages. Using typical email costs as a guide, this translates to a savings of $900,000, providing an immense return on investment.[2]

ISPs and other receiving networks benefit by avoiding the risk of inadvertently deleting email their users want and reducing the cost of managing a list of approved senders, often referred to as a "whitelist." Consumers gain a more trustworthy communication channel, where transaction receipts, requested newsletters, customer service responses, and other communications from certified senders are reliably delivered.

## Bonded Sender Program Requirements for Email Senders

To become a Bonded Sender, originators of legitimate email are required to (1) complete a certification process to ensure they adhere to a set of email communication standards; and (2) post a financial bond to guarantee the integrity of their email campaigns.

1. *TRUSTe Certification*. Independent, third party oversight of the Bonded Sender Program is provided by TRUSTe, a non-profit organization dedicated to enabling individuals and organizations to establish trusting relationships over the Internet. To join Bonded Sender, email senders must adhere to a baseline set of industry standards for email communication established by TRUSTe. TRUSTe also certifies senders and provides oversight and dispute resolution services for Bonded Sender, including monitoring complaint rates and auditing compliance with program standards.
2. *Bond*. To ensure the ongoing integrity of email sent by Bonded Senders, senders must post a financial bond. The size of the bond will vary based on the volume of email sent. Should end-users complain about the traffic they receive from a Bonded Sender above a specified threshold, a debit is made against the bond. This market-based mechanism provides ISPs and email administrators with an objective way to ensure that traffic passed directly on to end-users mailboxes comes from a qualified sender who will stand behind the email it sends. For a responsible email sender, the cost of the Bonded Sender Program is minimal.

## One Year Later: Lessons Learned from the Bonded Sender Experience

### Lesson #1: Incentives for good behavior in email work.

The Bonded Sender Program combines an enforcement mechanism (bond debits) with an incentive for good behavior (increased deliverability to participating networks). This "carrot and stick" approach is a powerful model that has greatly increased the value proposition to senders. The program sets a bar for email sender behavior and holds out a compelling additional value for those that clear the bar. Perhaps more importantly, the program adds a new dynamic to the email landscape that had not before existed in a compelling form: an opportunity for email senders to establish themselves as part of a new class of a legitimate senders that adhere to best practices and are rewarded accordingly with special delivery privileges.

In TRUSTe's experience as the certification authority for the Bonded Sender Program, the incentive-based approach attracts a much higher caliber of sender and motivates borderline senders to improve. Senders on the cusp of acceptance into the program regularly improve practices and resubmit themselves to TRUSTe scrutiny to gain the benefits promised by the program. The incentive has also allowed TRUSTe to highlight the importance of good practices for the industry, and to encourage bottom-line focused organizations to move to the top quartile of privacy practices in email, where they may have been previously focused on simply avoiding the bottom quartile, where anti-spam solutions have focused their consequences. Ultimately, TRUSTe believes that the incentives this

2. Complete case study: <http://www.bondedsender.com/media/090204_CNET_CaseStudy.pdf>.

approach provides for online emailers to adhere to high standards of behavior will move the needle of the industry towards better practices overall.

## Lesson #2: Sender company email policy matters.

The Bonded Sender Program relies heavily on keeping track of the number of complaints lodged against a participant as a measure of the compliance of participating senders with program requirements. TRUSTe believes that complaint rate is a vitally important metric, but it is insufficient when used in isolation to determine an email sender's trustworthiness. Complaint rate alone, like any reputation score that is automatically generated without human evaluation, has many shortcomings.

1. It provides no indication of compliance with legislated standards of behavior.
    - A low complaint rate, for example, does not mean that a sender is compliant with even the most basic provisions of the CAN-SPAM act.
2. It provides no assurance that standards for consent (a request from the consumer to receive such mailings) or disclosure (for example, of data sharing practices) have been met.
    - Reasonable protocols for consent and disclosure are among the most critical ways an email sender can establish a credible relationship with consumers.
3. Many senders are unfairly penalized.
    - This is particularly true for senders with new brands not yet widely recognized by consumers and senders in sensitive industries.
4. Complaint rates are not a reliable differentiator at the margins.
    - Example: The bottom decile of most mathematically generated reputation scores will usually feature reliably undeliverable senders, but there is no transparent or generally understood explanation for the difference between second and third deciles. For this reason, reputation scores tend to be better at eliminating "black hat" spammers than understanding where to draw the line among the myriad of "gray" senders.
5. The complaint rate does not reflect some of most egregious practices in email.
    - Example: An email address collector can share addresses with an unlimited number of outside marketers using no consumer disclosure, and that collector's individual reputation, as measured by traditional reputation scoring systems, will never be adversely effected.

The Bonded Sender Program acknowledged from the outset that complaint rate alone would not be enough to ensure a roster of high quality senders. For legitimate senders to be viable on the market, those senders must adhere to a company email policy founded on a clear baseline of good practices, and measures must be in place to ensure that senders remain at or above that baseline over time. TRUSTe has many methods for ensuring this compliance, from having applicants fill out a legally binding self assessment and cross referencing this with consumer disclosures and others materials, including privacy statements and terms and conditions, to personally testing unsubscribe links and seeding applicant lists. The strength of the policy component of the program, which has been TRUSTe's specialty, is a major reason that many leading receiving networks, including Hotmail, MSN, RoadRunner, and Outblaze, have faith in the Bonded Sender Program.

## Lesson #3: An Independent Trust Authority effectively complements government enforcement.

Through the Bonded Sender Program, TRUSTe closely monitors the behavior of over 130 email senders, including many prominent consumer brands and high volume email marketers. TRUSTe monitors complaint rates on a weekly basis, inspects emails sent to seeded lists, and conducts periodic reviews of participating companies' email policies. These measures, when combined with the carrot and stick approach of the program, provide real incentives for email senders to adhere to industry best practices. An Independent Trust Authority is able to apply a level of scrutiny to its participating senders that government is not able apply, except in very focused investigations. Furthermore, an Independent Trust Authority extends the power of government enforcement agencies by freeing such resources to focus on the most egregious offenders. TRUSTe has served, and will continue to serve in the Bonded Sender Program and others, as a first line of defense for email consumers.

# Moving Forward: A Consumer-Facing Seal and an Accreditation Policy Framework

## A Consumer-facing Seal

Thus far, TRUSTe has been accrediting email senders solely for the benefit of the Bonded Sender Program. But our certification process includes a thorough review of the sender's overall history and current practices, which prepares us to provide additional services to both the sender and affected consumers. At its core, the Bonded Sender Program is strictly a business-to-business whitelisting service, with no consumer-facing communication mechanism. In early 2005, TRUSTe intends to launch a point-of-collection, web-based seal program for accredited senders. Our research, including the disputes consumers submit directly to us through our web seal program, have consistently indicated that spam is the top concern of consumers on the Internet, and that this concern is materially limiting e-commerce. This new program will provide a trust mark for the online forms accredited senders use to collect email addresses. The trust mark will reassure consumers that they are interacting with a company that will not abuse their email address. The program will leverage similar certification procedures to the Bonded Sender Program and will include ongoing monitoring and enforcement mechanisms.

TRUSTe is pursuing additional email accreditation strategies and is exploring several key partnerships with leading email technology companies, who look to TRUSTe for guidance and expertise. In its research, TRUSTe has amassed a broad understanding of the full range of available and emerging technologies and standards. TRUSTe is a highly respected contributor to the Anti-Phishing Working Group ("APWG") and the Sender ID Framework initiatives as well.

## The Emerging Landscape: Support for an Accreditation Policy Framework

In the anti-spam context, "authentication" usually refers to a breed of Internet protocols designed to prevent specific forms of sender identity spoofing commonly used by spammers. The adoption of authentication is the first in a series of steps that industry is expected to undertake to provide receiving networks with the information they need to effectively block spam from recipients' inboxes. The adoption of authentication will affect the email infrastructure substantially, and will extend the opportunity for TRUSTe to play a material role as an Independent Trust Authority. In the Project Lumos White Paper,[3] the Email Service Providers Coalition presents one of the more developed models for reputation and accreditation (or certification) services in an authenticated environment.

TRUSTe describes the three emerging tools for receiving networks in the war against spam as follows:

- **Authentication** of sender identity: Authentication establishes a validated connection between the sending IP address and the domain asserted as the sending domain. (Non-IP systems are also in discussion.) This can be enhanced with a connection between domain and physical entity, as in the case of Verisign's validated domains list.

- **Reputation** of sender: Reputation services use numeric scoring systems to measure sender quality. Common data inputs include mail volume, complaint rate, abuse history, quality of DNS records, list hygiene, etc. Among the advantages of a reputation service is its ability to react quickly to behavioral changes, and data to make available on all senders, not just manually reviewed senders. Among its disadvantages is that it tends to be much more helpful in identifying black hat spammers. Within gray areas, a score can be a poor accounting and often misses critical factors like legal compliance, third party sharing, natural variations across industries, etc. Reputation services can cripple well-intentioned companies that would like to improve. New companies will have no reputation.

- **Accreditation** of sender: Accreditation services conduct a thorough review of sender's compliance with a transparent set of email policy standards. Standards would include permission level, quality of consumer disclosures, sharing practices, etc. In certain accreditation models, a sender can self-accredit, volunteering its standards in a public record according to a commonly accepted format. Senders can also seek accreditation by an independent third party, providing obvious credibility advantages. Third parties would provide ongoing monitoring and enforcement to ensure continued compliance over time and dispute

3. Project Lumos white paper: <http://www.projectlumos.com/lumos_white_paper.php>.

resolution services to provide program accountability.

It is important to recognize that these three sets of information are complementary, not competitive. Together, they provide a receiving network with the following:

- the confirmed identity of the sender;
- assurance that the sender does not have an egregious sending history; and
- assurance that the sender abides by a set of business practices consistent with the law and the reasonable expectations of the end users of their network.

In keeping with this framework, the leading authentication standards have been designed such that they provide an excellent technological platform to make additional statements, particularly about the sender's email policy and its status with accreditation authorities. Sender ID requires the sender to publish an SPF record in the DNS records. This record can easily be extended. DomainKeys requires the sender to publish a public key in the DNS. With receivers checking this record for key matches, it again provides a logical point of extension. The Internet drafts for both specifications refer explicitly to the role of authentication not as a stand-alone cure for spam, but as a cure for forged identity email and a foundation for the additional data points that receiving networks require to effectively combat spam. For these reasons, TRUSTe is confident that the current momentum for authentication within the industry will soon be followed by demand for a new breed of reputation and accreditation services. As the preeminent email accreditation service provider, TRUSTe has a strong desire to make a sender's email policy more transparent, elevating senders adhering to higher standards and providing a powerful incentive for others. To this end, TRUSTe leads the development of an accreditation policy framework that would build on authentication protocols, adding a sender's email policy. These policy data points would include attributes with which a consumer is most concerned (disclosures, the right to unsubscribe, level of commercial content, etc.). The information would be provided in detail to receiving networks, and potentially to email consumers as well. When a sender's email policy can be published in a reliable format, and receiving networks, on behalf of their consumers, can screen incoming mail against policy preferences, a far more reliable email network will be born.

TRUSTe will continue to play an influential role in the market in 2005, advocating for the necessary infrastructure evolutions and lending our expertise in developing operational email policy for companies. In the future, this effort to make policy a standardized and reliable data input for mail screening could become the most important aspect of TRUSTe's role as an Independent Trust Authority.

# Section 3 - Enforcement of the CAN-SPAM Act

# The CAN-SPAM Act: Overview of Anti-Spam Enforcement in 2004

*Charles Curran*
*Assistant General Counsel, America Online, Inc.*

*Jennifer Archie*
*Latham & Watkins*

To the surprise of no one, including the sponsors of the law, the passage of a federal law providing enhanced penalties for spam abuses did not result in an overnight halt to the billions of junk email messages sent every day through various tactics of technical falsification. Yet from a civil and criminal law enforcement perspective, CAN-SPAM has delivered a much more effective arsenal of enforcement tools that are now being used to help turn the tide in the war on spam.

Since the passage of CAN-SPAM, federal and state enforcement agencies have significantly enhanced their cooperation with Internet Service Providers (ISPs), and this cooperation is now producing tangible results. Government and industry are working together much more closely to quickly identify high-volume spammers, catch them in the act of spamming, and hold them accountable. ISPs contribute their expertise in deciphering the Internet routing and content of spam messages, and help cull through millions of fraudulent messages to uncover the identities of spam "kingpins" who use ever more sophisticated tactics of technical evasion to hide their tracks. Federal and state enforcement agencies, with their deep experience in "following the money" in other fraud matters, can now leverage both technical and financial evidence to assemble effective prosecutions that take advantage of the strong remedies in CAN-SPAM. Most significantly to the longer-term effectiveness of the Act, there is a far greater exchange of information about emerging, "state-of-the-art" techniques of spamming (including, for example, the viruses used to compromise servers in connection with spam-related activity), coupled with greater technological sophistication by government investigators concerning these spammers' tactics.

Four recent cases under the CAN-SPAM Act demonstrate the effectiveness of the statute as an enforcement tool, across a variety of different spam-related fact patterns:

- In April 2004, just four months after the passage of CAN-SPAM Act, the U.S. Attorney for the Eastern District of Michigan arrested and filed criminal charges against four alleged spammers. The complaint charged these individuals not only with disseminating fraudulent weight loss products, but also with having falsified email transmission information in violation of the CAN-SPAM Act.

- In June 2004, the U.S. Attorney for the Southern District of New York indicted two individuals under the CAN-SPAM Act for the theft of a list of millions of AOL email addresses that was sold to and used by spammers.

- In July 2004, the Attorney General of Massachusetts filed civil claims under CAN-SPAM against a company for allegedly sending spam advertisements for mortgage rates with misleading header information, as well as other violations of other CAN-SPAM Act requirements.

- In September 2004, a man pled guilty in federal court in California to charges under the CAN-SPAM Act that he exploited unsecured WIFI servers to transmit pornographic spam.

Some might attempt to dismiss the 2004 cases as isolated examples of enforcement activity not having a real impact on spamming behavior. But these cases must also be viewed against the backdrop of an enforcement reality in which the development of a criminal case against a significant spammer may sometimes take time – and in which much of the deterrent value of anti-spam legislation is linked to actual convictions. This point is well illustrated by the Commonwealth of Virginia's experience with its first-in-the-nation felony anti-spam law. In July 2003, six months prior to the passage of CAN-SPAM, Virginia established felony-level penalties for header falsification in spam transmission. Just five months later, in December 2003, following an expedited investigation, a Loudoun County grand jury indicted Jeremy Jaynes (considered the eighth-largest spam distributor in the world by the anti-spam organization Spamhaus). Although Jaynes' trial did not take place until ten months later (October 2004), the outcome

was successful for Virginia's anti-spam prosecution team. Following an eight-day trial, Jaynes was convicted of three felony charges of fraudulent spam transmission. Significantly, the jury recommended a sentence of *nine years* in prison for Jaynes.

The Jaynes case illustrates not only the type of timeline between the criminal conduct and ultimate conviction of a large-scale spammer, but also how vigorous prosecution is necessary to truly deter large scale spammers. The testimony in the case showed that Jaynes transmitted his spam to Virginia knowing full well about its new anti-spam law, under the misimpression that no prosecutor would pursue a detailed investigation to hold him accountable for his actions. The publicity surrounding the jury's nine year prison sentence recommendation for Jaynes may provide a far more significant deterrent to other spammers wondering about their chances under newly-minted anti-spam legislation, including CAN-SPAM. These spammers will understand that there will soon be many more cases under CAN-SPAM and similar anti-spam legislation, and that these cases will be pursued vigorously.

Private ISPs have, of course, been extremely active in 2004 in bringing actions that take advantage of the robust civil remedies under CAN-SPAM. Four major U.S.-based ISPs – AOL, Microsoft, Yahoo, and Earthlink – filed the first civil CAN-SPAM suits in March 2004 against hundreds of as yet unknown (or "John Doe") defendants, as well as numerous named defendants. These lawsuits seek per-email penalties of at least $25 under CAN-SPAM, which as a practical matter would likely bankrupt any of the defendants. A second round of industry-coordinated CAN-SPAM suits was announced in October 2004, against defendants advertising online pharmacies, mortgages, debt relief and adult websites, among other products and services. All of these cases are on track to result in very significant settlements and judgments against the defendants in the near future.

Sustained effort by government enforcement agencies and industry under the CAN-SPAM Act will be necessary to achieve the maximum possible deterrence to the "outlaw" tactics of high-volume spammers. And, as acknowledged within the body of the Act itself, legal remedies can only play a partial role in any long term solution to the spam problem. Vigorous enforcement efforts must be complemented by continuing focus on improved technologies and consumer education. The new anti-spam technologies discussed at the FTC's November 2004 Email Authentication hold the prospect of eliminating many of the favorite tricks in the spammer's "toolbox," such as spammers' ability to "spoof" the domains and email addresses of innocent third parties. In the meantime, though, the enforcement tools provided under the CAN-SPAM Act have made possible significant successes in 2004 and beyond.

# Section 4 - Views from Europe

# European Union vs. Spam: A Legal Response

*Nicola Lugaresi*
*Associate Professor*
*Trento University, Law School*
*lugaresi -at- jus.unitn.it*

## Introduction

Unsolicited commercial communications now represent more than fifty per cent of the email traffic in the European Union and around the world. This paper is about the EU legal approach to addressing the problem of spam. Through the analysis of the evolution of the European legislative framework, it aims to define, from a legal perspective, why the opt-in choice has been adopted by the EU and the role of other anti-spam tools in addressing the problem.

The main reason why the European Union has addressed spam (assuming that spam is synonymous with unsolicited commercial electronic communications) is that spam affects fundamental rights of the individual. Not only is spam a global nuisance, but it concerns primarily people's privacy. It infringes the more visible side of privacy- the protection of personal data - as it involves not only the unfair and unlawful collection and use of private email addresses, but also illegal intrusion into computers and servers. Moreover, spam violates privacy in its broader and more sensitive sense - the "right to be let alone" - by filling in-boxes with loads of unwanted email. In this respect, spam deprives individuals both of their capacity to control the amount of personal information to be known by others and of their capacity to control the flow of information entering their private sphere.

Legal intervention to curb the flow of unsolicited commercial communications is therefore justified for several reasons, and is aimed to protect several interests, as EU Directives and other official EU documents acknowledge. Spam affects individuals, users, subscribers, consumers, companies, direct marketers, Internet service providers, traders, employers, organizations, public bodies and, in the end, the Internet itself. The EU has for several years been aware of the risks to users' privacy raised by the public availability of electronic communications services over the Internet.[1] And the EU has been aware that spam compromises electronic communications, interactive networks, terminal equipment,[2] productivity at work[3] and e-commerce itself.[4] Moreover, spam is often the means through which fraud is perpetrated, and the carrier of pornographic messages, hate speech and viruses.

EU laws alone are not likely to solve the problem, for both jurisdictional and technical reasons. Notwithstanding the ineluctability, in the short-term, of spam, the EU could not refrain from intervening to protect a repeatedly violated fundamental right. EU laws focus on two goals -the practical goal of reducing the amount of spam, and the ethical goal of attempting to guarantee the individual's control over personal relationships and contacts, both inbound and outbound. Unless legal regimes are coordinated and jurisdictional issues are resolved, the extent to which the first of these goals can be realized is substantially limited. With respect to the second, EU laws characterize privacy as a fundamental right, in all personal life expressions,[5] and identify spam as a major problem that plays a critical role in market failures, unless strict rules are enacted and enforced. Such an approach was encouraged by the recognition of the role of commercial communications in the information society.[6]

EU Directives apply to all unsolicited commercial communications received on and sent from networks in the European Union.[7] When email is originated in third countries, enforcement (and, in particular, the identification of spammers) is quite complicated, due to the limited experience of investigators and jurisdictional obstacles. Jurisdictional issues clearly show the need for international cooperation. In these terms, European Union legal strategies and corresponding

1. Article 1, and recital 6, Dir. 2002/58/EC.

2. Recital 30, Dir.2000/31/EC; recital 40, Dir.2002/58/EC.

3. EC Communication on "spam" (2004), §1.2.

4. Recital 60, Dir.2000/31/EC.

5. Council Decision 1999/168/EC (Annex II, §a.i).

6. Recital 29, Dir. 2000/31/EC.

7. EC Communication on "spam" (2004), §3.5.1.

laws must be regarded not as the ultimate answer to spam, but as an attempt to set up a rational discipline and as a possible model for a harmonized approach to reducing spam that rests on three elements.

First, law enforcement bodies must make a serious commitment to enforcing laws through adequate actions: effective penalties, national and cross-borders complaints mechanisms and remedies, monitoring, coordination among national authorities, international cooperation, and available resources. Spam must be fought, not just denigrated.

Second, regimes to control spam must come in different forms - legislation, self-regulation, architecture, and alternative dispute resolution - methods characterized by their flexibility and capacity to promptly adapt to new cases and technologies. Spam must be fought with a combination of weapons.

Third, social awareness of spam, the online behaviors that cause it, and the tools available to avoid it must be spread and reinforced, taking the form of education of users and market players, information, self-help, and the involvement of associations and privacy advocates.[8] Spam must be fought by all the actors involved.

## From Opt-out to Opt-in

Apart from broad political strategies, EU Directives on privacy, trade and communications have affected, since 1995, the way in which the problem of spam has been addressed. The early interest was motivated by the need to protect citizens and consumers from "high-pressure selling methods"[9] and from "certain particularly intrusive means of communication."[10] Unlike the CAN-SPAM Act of 2003 in the United States, however, the EU has not passed legislation specifically designed to combat the spam problem.

Directive 95/46/EC (Framework Data Protection Directive) does not deal specifically with electronic communications. Nevertheless, its provisions about the processing of personal data may provide mistakenly neglected and underestimated tools to combat spam. Email addresses are considered "personal data,"[11] which means that the manner in which they are processed must respect the rules set up by the Directive. Among other things, freely given, informed, specific[12] and unambiguous[13] consent must be provided by the addressee before the address is collected; principles of fair processing practices must be adopted;[14] collectors of email addresses must specify explicit and legitimate collection purposes;[15] and adequate information about the collection and use of the email address must be provided to the addressee.[16] In particular, for instance, activities such as the harvesting of email addresses on public Internet places as websites, chat rooms, newsgroups and so on, are illegal under the terms of the Directive 95/46/EC, constituting unfair processing of personal data, and violating both the purpose limitation principle and the obligation of adequate information principle mentioned above.[17] Similarly, implied consent, use of pre-checked boxes, and broad general requests for consent would not meet the requirements of the Directive with respect to transparency and fairness.[18]

Apart from the indirect protection provided by Directive 95/46/EC, the first tentative and implicit legislative reference to spam is contained in Directive 97/7/EC (Distance Contracts Directive). While the terms of the Directive require prior consent with respect to automated calling systems and facsimile machines,[19] for other "means of distance communication" (like email) it states that they can be used only where there is no "clear objection" from the consumer.[20] The Directive 97/7/EC does not define what a "clear objection" is, implicitly suggesting an opt-out system. Similarly, Directive 97/66/EC (Telecommunications Sector Privacy Directive), no longer in force, confirmed the opt-in rule only with regard to automated calling systems without human intervention or fax machines for the purposes of direct marketing.[21] For other means, like email, Member States were required

8. EC Communication on "spam" (2004), §3-5.
9. Recital 5, Dir. 97//7/EC.
10. Recital 17, Dir. 97//7/EC.
11. Article 2(a), Dir.95/46/EC.
12. Article 2(h), Dir. 95/46/EC.
13. Article 7(a), Dir. 95/46/EC.
14. Article 6(a), Dir. 95/46/EC.
15. Article 6(b), Dir. 95/46/EC.
16. Artt.10, 11, Dir. 95/46/EC.
17. DPWP, Working Document - Privacy on the Internet (2000), Chapter 4, §IV; DPWP, Recommendation 2/2001, §28.
19. Article 10(1), Dir. 97/7/EC.
20. Article 10(2), Dir. 97/7/EC.
21. Article 12(1), Dir. 97/66/EC.

to take "appropriate measures" to ensure that, free of charge, unsolicited calls were not allowed, which left national legislation free to determine whether to rely on opt-in, opt-out, or a mixed system.[22] Not surprisingly, Directive 2000/31/EC (Electronic Commerce Directive), took for granted that Member States could adopt opt-out systems for unsolicited commercial communications by electronic mail.[23] The opt-in system adopted for automated telephone calling systems and facsimile machines was not imposed on email, under a confirmed, but questionable, distinction. Directive 2002/58/EC (Electronic Communications Privacy Directive), which repeals Directive 97/66/EC, finally overcomes the doubts and the resistance about the adoption of a consent-based marketing system for email.[24] The individual's interest in being spared unsolicited commercial information was finally deemed to be more relevant than the concern that opt-in could hinder the development of e-commerce, discriminating against companies in the EU and possibly driving direct marketers to shift their activities outside of the European Union.

## The Manner of Consent

The opt-in system chosen by the Electronic Communications Privacy Directive of 2002 represents the arrival point of EU regulations on unsolicited commercial communications. The legislators thought that opt-in could more effectively protect individuals and better meet the expectations of users, Internet service providers and industry.[25] Moreover, an opt-in system requires a simpler legislative framework, is more easily implemented, allows more efficient advertising,[26] and, at least theoretically, ensures stricter rules, more likely to curb spam. According to article 13 of Directive 2002/58/EC, the use of "electronic mail for the purposes of direct marketing may only be allowed with respect to subscribers who have given their prior consent."[27] The opt-in "radical" choice is clear. Nevertheless, Directive 2002/58/EC introduces some succinct rules and some exceptions to a straight opt-in model that reveal some heritage of the previous opt-out system.

An interpretative issue may be raised by email addresses not associated with a subscriber, like addresses provided by companies or within a family. In these cases, as the prior consent must be given by the subscriber, the alternative to a lack of protection is represented by the consent given by the subscriber[28] who is not, on the other hand, the actual user.[29] But, as email addresses are personal data, it follows that an autonomous protection derives from the Framework Data Protection Directive of 1995.[30] Even if the address is not associated with a subscriber, and therefore protected by Directive 2002/58/EC, it is associated with the user, and therefore protected by Directive 95/46/EC.

An analogous issue may be related to email addresses contained in a mailing list. It may be argued that the prior consent must be given by the list-owner, which means that participants in the list may protect their privacy only by unsubscribing from the list. Alternatively, it may be maintained that each participant may block unsolicited commercial communications for the whole list. Unless technical solutions allow separate management of each email address on the list, with respective preferences, the answer depends on the choice about who is to be protected, and on the distinction between a contractual vision (the subscriber to the communication service, the list owner) and a more personal vision (the user of the service, the list participant).

Electronic contact details, obtained from customers in the context of the sale of a product or a service, may be used for direct marketing of similar products or services.[31] This approach has been characterized as a "soft opt-in." The opt-in may not, in fact, be that soft, as customers must be given the opportunity to object, free of charge and in an easy manner, to the use of their details both when they are collected and on the occasion of each subsequent direct marketing message.[32] Together with the electronic details, the consent of the user is collected. The real difference between "soft" and "hard" opt-in is the factual circumstance of the collection of the consent - a sale - but in both cases data must be obtained in accordance with the Framework Data Protection Directive

22. Article 12(2), Dir. 97/66/EC.
23. Article 7(2), and recital 14, Dir. 2000/31/EC.
24. DPWP, Opinion 7/2000, §2, comment to article 13.
25. DPWP, Opinion 7/2000, §2, comment to article 13.
26. Commission – Summary of Study Findings (2001).
27. Article 13(1), Dir. 2002/58/EC; recital 17, Dir. 2002/58/EC.
28. Article 2(k), Dir. 2002/21/EC.
29. Article 2(a), Dir.2002/58/EC.
30. DPWP, Opinion 5/2004, §3.4.
31. Article 13(2), Dir. 2002/58/EC.
32. Recital 41, Dir. 2002/58/EC.

of 1995. In fact, the chance to object to such use is necessarily related to the provision of adequate information on the use itself. The "previous sale" exception is therefore limited in several ways, and it must be interpreted restrictively.[33] There must have been a "sale," not just a vague commercial relationship; the use of electronic contact details is limited to the "same company," which rules out subsidiaries or mother companies;[34] and direct marketing must be limited to "similar" products or services, where similarity should be judged from the reasonable expectations of the recipient.[35] In these terms, if correctly applied, the collection of the electronic details in the context of a sale represents an alternative method to negotiate, and possibly obtain, prior consent for commercial communications.

Directive 2002/58/EC prohibits the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender, or without a valid address where the recipient can exercise the opt-out.[36] Such a prohibition is motivated by effective enforcement of EC rules,[37] but it sounds somehow redundant, as unsolicited communications are prohibited in any case. In an opt-out approach, disguising or concealing identities and return addresses would make a commercial communication illegal. In an opt-in setting, it would mainly reinforce the degree of illegality. It is possible, but unlikely, that a sender who has obtained a valid prior consent violates the provision. It is more likely that disguising or concealing occurs when the sender has not obtained valid consent. Moreover, the "disguising and concealing" violates, again, the Framework Data Protection Directive of 1995, as others' personal data are processed without consent.

Finally, Directive 2002/58/EC states that the opt-in system applies to natural persons only. As for legal persons, Member States must ensure sufficient protection of "subscribers other than natural persons" from spam.[38] While the legal distinction between natural and legal persons looks clear, compliance by senders with two different systems -opt-in for natural persons, opt-out for legal persons - may not be that easy. Email addresses do not always show whether the recipient is a natural person or a legal person. In these terms, the sender must carefully verify the nature of the recipient[39] or risk engaging in an illegal activity. Including legal persons in a compulsory opt-in scheme might be a rational and simplifying choice.

## The Ancillary Tools

Notwithstanding the adoption of an opt-in system, the EU Directives in force contain some provisions setting up tools that might be used in conjunction with opt-out systems.

### Filtering and Labeling

EU Directives take into consideration filtering and labeling as tools useful for better implementation, and in particular to avoid the costs that spam imposes for the recipient. Thus, the Electronic Communications Privacy Directive of 2002 promotes and encourages industry filtering initiatives[40] through email systems arrangements that allow subscribers to view the sender and the subject line of an email and to delete messages without having to download the content or attachments.[41] This means that Member States must ensure that such commercial communication by a service provider established in their territory is clearly and unambiguously identifiable as such "as soon as it is received by the recipient,"[42] for instance with an "ADV" label in the subject line. Apart from issues about free expression and forced speech that are more sensitive in the US than in the EU, an "ADV" label functions more coherently with an opt-out system, in which different kinds of commercial communications can be received. In an opt-in system, the commercial communications received either is legitimate, and solicited, with a prior consent, or is illegal, in which case the label would not make it legal.

Directive 2002/58/EC leaves the protection of the legitimate interests of legal persons to Member States, which must ensure sufficient protection. The Directive may, in fact, establish an opt-out registry for spam,[43] which is not compatible with an opt-in system. "Opt-out registers" (or "Do Not Email lists") were already considered by the Electronic Commerce

33. DPWP, Opinion 5/2004, §3.5.

34. DPWP, Opinion 5/2004, §3.5.

35. DPWP, Opinion 5/2004, §3.5.

36. Article 13(4), Dir. 2002/58/EC.

37. Recital 43, Dir. 2002/58/EC.

38. Article 13(5), Dir. 2002/58/EC.

39. DPWP, Opinion 5/2004, §3.4.

40. Recital 30, Dir.2000/31/EC.

41. Recital 44, Dir. 2002/58/EC.

42. Article 7, Dir. 2000/31/EC.

Directive of 2000, which required service providers undertaking unsolicited commercial communications by electronic mail to consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications could register themselves.[44] Besides, "Do Not Email lists" may pose a threat to users' privacy unless created as domain level registries. Email address-based registers that collect and possibly disclose individual email addresses threaten privacy rather than protect it. Moreover, particularly considering cross-border activities, they may involve burdensome activities for users (especially if they change regularly their email addresses, possibly as a self-help measure against spam), for direct marketers (who should constantly check them), and for authorities or organizations charged to manage and keep them up-to-date. Apart from security concerns, the risk is to end up with a Big Brother, or many scarcely known Smaller Brothers, which would make it even harder for users to orientate and for direct marketers to comply.

### Codes of Conduct and Self-regulation

Codes of conduct are another tool considered by the Directives, and they have been promoted since Directive 95/46/EC.[45] Before Directive 2002/58/EC, self-regulation had been considered the main regulatory instrument for fighting spam.[46] Directive 2000/31/EC encourages "professional associations and bodies to establish codes of conduct at Community level in order to determine the types of information that can be given for the purposes of commercial communication".[47] The same Directive tries to make codes of conduct more transparent, favoring the voluntary dissemination of draft codes of conduct, the accessibility of them by the public, and the "involvement of associations or organisations representing consumers in the drafting and implementation of codes of conduct affecting their interests."[48] Evidence showed that self-regulation alone, even if subjected to procedural steps aimed at making it more reliable[49] and transparent, failed. While self-regulation intended as self-limitation is clearly not suitable to discipline as sensitive a matter as spam, even self-regulation intended as participated co-regulation cannot be the only regulatory reference, and legislation is needed, especially to make enforcement possible. Again, self-regulation, codes of conduct, quality labels and good marketing practices are far less necessary in an opt-in system than in an opt-out system, as an opt-in approach is a more autonomous, complete and enforceable approach than opt-out.

### "Spam Boxes"

While EU Directives do not cite "spam boxes" as possible tools, some national Data Protection Authorities (DPA)[50] have adopted such initiatives, backed by other official EU documents. Users may forward the spam they receive to spam boxes, created by DPAs, activating enforcement mechanisms. Even spam boxes that do not employ bounties encourage consumers to report infringements, favoring a more diffused and effective enforcement of adopted legislation, and providing DPAs with data and statistics. Spam boxes are an easy, direct and cheap way of complaining and reporting violations, a sort of "one click away" hotline. The user need only forward the unwanted spam to the spam box and is not required to explain, either in writing or by telephone, how the spam occurred.

### Contracts

Finally, contracts can be of help in the fight against spam, through the adaptation of terms and conditions of subscriber contracts to the opt-in system. Internet service providers (ISPs), email service providers (ESPs), and providers of mobile services should include obligations in contracts prohibiting the use of their services for sending spam, and provide information on anti-spam filters and other tools that can be used by subscribers to control spam.[50] Effective contractual penalties should be set up in case of breach.

## Conclusion

The evolution of the EU legal system shows how self-regulation and an opt-out system failed in curbing spam. The opt-in choice, adopted by Electronic Communications Privacy Directive of 2002, is the re-

43. Article 13(5), Dir. 2002/58/EC; recital 44, Dir. 2002/58/EC.

44. Article 7(2), Dir.2000/31/EC; recital 31, Dir. 2002/58/EC.

45. Article 27, Dir. 95/46/EC.

46. Recital 32, Dir.2000/31/EC; see also recital 41, Dir.2000/31/EC.

47. Article 8(2), Dir.2000/31/EC.

48. Article 16(2), Dir. 2000/31/EC.

49. DPWP, Opinion 3/2003; see also article 30, Dir. 95/46/EC.

50. For instance, by the French 'Commission Nationale Informatique et Libertés (CNIL)' and the Belgian 'Commission de laProtection de la Vie Privée(CPVP).

sponse EU considers more rational, proper, effective and respectful of the main interest to be protected: the individual's privacy. This rules out neither the need to sign international agreements, in order to coordinate different systems (opt-in and opt-out), nor reliance on other regulatory tools (as law alone is not sufficient). EU regulates, and puts forward a policy proposal at the same time. As for article 13 of the Directive 2002/58/EC, which contains the basic rules on unsolicited commercial communications, it shows how some traces of the previous opt-out system have survived, making the discipline somehow less coherent in some parts. Finally, there is a need to define what spam is, as the frequently used term "spam" is not a legal term, which may involve some misunderstandings about the real object of the discipline.

# References (EU Materials)

### EU Directives and Decisions:


- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data <http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett>.

- Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts <http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31997L0007&model=guichett>.

- Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector <http://europa.eu.int/eur-lex/pri/en/oj/dat/1998/l_024/l_02419980130en00010008.pdf>.

- 1999/168/EC: Council Decision of 25 January 1999 adopting a specific programme for research, technological development and demonstration on a user- friendly information society (1998 to 2002) <http://europa.eu.int/eur-lex/pri/en/oj/dat/1999/l_064/l_06419990312en00200039.pdf>.

- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce") <http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf>.

- Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services ("Framework Directive") <http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_108/l_10820020424en00330050.pdf>.

- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ("Directive on privacy and electronic communications") <http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf>.


### Data Protection Working Party Documents:


- Data Protection Working Party - Opinion 7/2000 on the European Commission proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 (2 November 2000) <http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2000/wp36en.pdf>.

- Data Protection Working Party, Working Document, Privacy on the Internet – An Integrated EU Approach to On-line Data Protection (21 November 2000) <http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2000/wp37en.pdf>.

- Data Protection Working Party - Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union (17 May 2001) <http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2001/wp43en.pdf>.

- Data Protection Working Party - Opinion 3/2003 on the European code of conduct of FEDMA for the use of personal data in direct marketing (13

June 2003) <http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp77_en.pdf>.

- Data Protection Working Party - Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC (27 February 2004) <http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp90_en.pdf>.

### Other EU Documents:

- Commission of the European Communities - Unsolicited commercial communications and data protection – Summary of Study Findings – January 2001 <http://europa.eu.int/comm/internal_market/privacy/docs/studies/spamsum_en.pdf>.

- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on unsolicited commercial communications or "spam" (22 January 2004) <http://europa.eu.int/information_society/topics/ecomm/doc/useful_information/library/communic_reports/spam/spam_com_2004_28_en.pdf>.

# The experience of the European Union with the "opt-in" approach

*Miriam Rado*
*Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband)*
*http://www.vzbv.de*

With the E-Privacy directive of 2002 (2002/58/EC) the European Union established the principle of the "opt-in" approach for email advertising. All Member States are obliged to adopt this rule within their national legislation. The "opt-in" rule means that companies may send electronic communications for advertising purposes only when the recipient has given prior consent. Cases in which the advertiser has received the email address of a consumer in connection with the sale of a product or provision of a service are excepted from this rule. In these cases the advertiser may use the address for direct advertising of similar goods and services, under certain conditions.

The question of "opt-in" versus "opt-out" centers on weighing consumers' right to privacy against companies' interest in marketing their products freely to individual consumers. The European view is that there is no right of businesses to contact any individual unless the individual has explicitly authorized the receipt of commercial messages. In the 2003 Transatlantic Consumer Dialog (TACD) survey, more than 80 percent of the participants called for a clear opt-in approach. US participants voted in the same manner as EU participants, suggesting that also US consumers do not see spam as a vehicle for "freedom of speech" but rather as annoying advertising.

Because spam is a serious problem for consumers and businesses, the business community also supports the "opt-in" approach. The EU Commission estimates economic damage of EURO 2.5 billion per year caused by spam through loss of productivity. Employee work hours spent disposing of their daily spam emails make up a significant amount of this damage. In addition, many businesses and enterprises in Europe use other kinds of advertising to address consumers, as they have discovered that spam damages their reputation, leading to a loss of consumer trust - one of the most serious economic threats posed by spam.[1]

1. In the TACD survey, more than half of the 20.000 participants said that they were very reluctant to shop online because they fear an increase of spam mails.

An opt-in approach offers several benefits.

*An opt-in approach aids law enforcement agents in determining and proving whether a spam mail is legal or not*. In an opt-in approach, the sender must prove the prior consent of the recipient. Also, when recipients exercise an opt-out, spammers are able to establish that an email address is valid.

*An opt-in approach, adopted by all countries, would facilitate cross border cooperation in enforcing anti-spam laws*. As the responsibilities and competences of enforcement agencies from different countries vary from one another, consistent classification of spam is essential. Investment in efforts to distinguish between legitimate spammers and illegitimate spammers weakens the fight against spam. International spam enforcement also encounters technical problems with detecting the actual sender and legal and practical problems related to the prosecution of spammers in foreign countries. The "opt-in" approach is the only international solution for legislation to overcome international barriers.

It is difficult to estimate the effectiveness of the "opt-in" approach in Germany as the opt-in approach had been adopted in the country even before the European legislation. There are no figures that measure spam "before and after" the establishment of "opt-in."

It should be noted, however, that even the "opt-in" approach has not solved the problem of spam in Europe completely, as spam continues to comprise a large portion of the messages in email boxes.

The "opt-out" approach does not only force consumers to react to every email they receive, it also ignores the existing problems with deceptive spam, as most deceptive spam looks as if it is respectable. As they cannot be detected as being deceptive immediately, it is very important that all spam mails can be tackled. While consumer organizations as well as governmental agencies try to educate consumers not to give out their email addresses to persons they do not know and not to click on any links in a spam email, this is exactly what is required by the CAN-SPAM Act.

According to the CAN-SPAM Act consumers can use a link to unsubscribe to spam and put their email address in the company's opt-out list. Fraudulent spammers could use advertising mails with these links for modem hijacking and for selling these lists to other spammers. There is no way for the consumer to find out whether the advertising mail comes from a reliable sender or not. A consumer who has once used the link in a spam mail and whose modem has been hijacked in that way will then lose his trust in any link and eventually in the Internet as a whole.

# Section 5 - Spam Solutions and Issues of Free Expression and Access to Email

# Non-commercial Email Lists: Collateral Damage in the Fight Against Spam

*Cindy Cohn, Legal Director*
*Annalee Newitz, Policy Analyst*
*Electronic Frontier Foundation*[1]
*http://www.eff.org*

## Introduction: Spam Solutions and the Free Expression Compromise

In their zeal to stop spam, many organizations and companies are blocking the delivery of wanted messages, especially those sent through email lists. The often-negative experiences of people depending on such email lists can be instructive for policy-makers and administrators who must determine how to handle spam filtering on a large computer network. Here we explore how these experiences reveal flaws in current anti-spam mechanisms – flaws that can and must be fixed, if we value freedom of expression online.

Let's begin by considering the case of MoveOn.org, a politically progressive organization that engages in online activism. For the most part, its work consists of sending out action alerts to its members via email lists. Often, these alerts will ask subscribers to send letters to their representatives about time-sensitive issues, or provide details about upcoming political events. Although people on the MoveOn.org email lists have specifically requested to receive these alerts, many large ISPs regularly block them because they assume bulk email is spam. As a result, concerned citizens do not receive timely news about political issues that they want. Often, MoveOn.org's staff doesn't discover that the mail isn't getting through for days or weeks, and even when it does, ISPs respond slowly to "unblock" requests or refuse to explain why email has been confiscated. Although ISPs may have the best of intentions, what this scenario – one that is all too common – represents is the chilling of free speech in the service of blocking spam.

This problem is exacerbated by the fact that most blocking processes are not transparent to the email sender or recipient, and email users are generally given little or no control over which emails are blocked. Instead, system administrators, creators of spam-blocking tools, and ISPs all too often attempt to predict what mail a recipient does and does not want. As a result, email users rarely receive all legitimate messages sent to them.

The large number of anti-spam tools is a tremendous problem for email list owners, who must navigate everything from "block lists" to Bayesian filters[2] to communicate with willing recipients. The fact that unwanted email often masquerades as wanted email complicates matters, as do the ongoing differences of opinion and policy about when a person has consented to be added to an email list. Some evidence also exists that administrators are misusing spam blockers to block email lists because of personal malice or political opposition to the content of the messages. This is clearly the case when email is administered under government regimes like the one in China.

Additionally, a growing number of proposals, loosely called "bonded sender" initiatives, require that organizations sending bulk email pay a fee to register with various "bonder" organizations. This practice might mean that groups that cannot pay will have their non-commercial email relegated to second-class status that slows its delivery. Indeed, expensive certification requirements and reflexive blocking of all "uncertified" email could mean that mail from non-commercial mailing lists won't be delivered at all.

When tools designed to prevent unwanted email also prevent wanted email from being delivered, or when anti-spam tools favor well-funded speakers over others, something fundamental to the health of Internet communication has been broken. Email is no longer a strong vehicle for free speech.

1. The Electronic Frontier Foundation (http://www.eff.org) is a member-supported, civil liberties organization working to protect rights in the digital world. Founded in 1990, EFF actively encourages and challenges industry and government to support free expression and privacy online.

2. A Bayesian filter uses statistical methods to analyze the text of an incoming email to determine the probability that it is a piece of spam. Probability is based the occurrences of certain words, often customized by the user.

In this paper, we introduce the major problems faced by senders and receivers of non-commercial bulk email, a group whose communications are the most threatened by anti-spam measures.

## Impeded Use of Non-Commercial Email Lists

Email lists are among the most important, powerful and accessible communication tools on the Internet, allowing a single person or group to send messages to a much larger group of people who have agreed to receive the messages. They allow recipients to learn about current issues and participate more easily in initiatives and events that they care about. Email lists help people to track government and world events minute-by-minute, and thereby participate in public debate in new and powerful ways. The topics addressed by non-commercial email lists are as diverse as human thought itself; there are lists devoted to such varied subjects as electoral politics, AIDS prevention, knitting and the San Francisco 49ers.

Yet developments in controlling the proliferation of spam place at risk the continued viability of email lists as cheap, efficient means of one-to-many communication. An informal survey conducted by EFF in 2003 revealed that many organizations with large email lists, and even some organizations with smaller ones, face an ongoing struggle to get email delivered to members. List owners for groups as small as the parents of Berkeley, California high school students and as large as Moveon.org, which has lists with two million subscribers, reported problems with anti-spam mechanisms. Other list owners negatively affected by these mechanisms include technologist and author Bruce Schneier, who publishes the highly respected Cryptogram newsletter, and the people behind TidBITS, a prominent email list for the Macintosh Internet community. EFF faces ongoing difficulties with anti-spam mechanisms in sending out our own long-running newsletter, EFFector.

Email list owners and recipients face multiple issues as a result of these mechanisms. Among these concerns are: a lack of transparency, or an inability to easily determine that one's email is being blocked, by whom it is blocked and why; unfair or poor rationales for blocking; a lack of due process for emailers whose messages are being blocked; and barriers to entry raised by bonded sender programs. The discussion below considers some of the major problems, although the list is by no means comprehensive.

## Lack of Transparency

We've found that by far the most common problem with email blocking is that it's difficult for members of an email list to figure out that they've stopped getting email from the list.

Recipients report that they don't notice that they've stopped receiving messages for several weeks or months, and often only after missing important ones. Similarly, email list owners say that it's hard to know when their messages have been blocked. Often, they only discover blocks when they receive angry or confused messages from subscribers who believe they've been dropped off a list intentionally or through negligence. Some blocks result in bounced messages to the email list owner, providing an explanation of what went wrong — but most blocks do not. And no email list owner or recipient is warned ahead of time that a message will be blocked, much less receives instructions about how to avoid it.

Even when an email-list member discovers that her mail is being blocked, it's often extremely difficult to find out who has blocked it and why. While her ISP is usually the direct cause of the block, ISPs generally use a software package or third-party anti-spam service such as MAPS or SpamCop,[3] and that list or mechanism is what determines whether or not a message is delivered. Tracking down the proprietors of blocking software and anti-spam services can be very difficult. ISPs are not usually forthcoming with the names of the various private services they use, even to subscribers, and anti-spam services rarely list their clients. Moreover, an anti-spam service often won't reveal its rationale for blocking certain senders, even to the ISPs with whom it does business. Thus, even if an ISP admin wanted to explain to a user why he hasn't received his email, often she can't.

These problems could be solved if ISPs or their third-party blocking services would send out bounce notifications to people sending email, or "email blocked" notices to recipients. If people are alerted in a timely fashion that their email is being blocked, the blocking process grows less opaque and steps may be taken to remedy the problem. To facilitate this process, bounce and block notices should contain a clear procedure for reporting the improper block.

3. For an explanation of how blocklists like MAPS work, see <http://www.scconsult.com/bill/dnsblhelp.html>.

## Free Speech Problems Raised by Common Methods of Blocking Email

Email is typically blocked for a few basic reasons, some more fair than others. Here we outline five techniques that inform email blocks. Many of them can lead – usually inadvertently – to situations where people aren't getting the emails they wish to receive. Other methods, especially ones that place control in the hands of users, seem less likely to result in mail being mis-categorized as spam.

### Probabilistic Classification/Machine Learning

Probabilistic classification is a family of techniques involving computer programs that "learn" what is and is not spam, allowing the programs to adapt over time. Using "machine learning" algorithms, the programs determine the probability that a given email should be classified as spam. The technique known as Bayesian filtering belongs to this group.

These algorithms must be "trained" with starter data before they can begin automatically classifying documents. Different learning algorithms achieve varying degrees of success, but most such algorithms improve as they are trained by users who mark certain mail as "spam" and other mail as "not spam." As a result, this technique can allow for significant end-user control, thus placing control of spam filtering in the right hands.

### Ad Hoc Pattern Matching

Many spam detectors search for specific spam-like patterns, such as all-caps or gappy text, words like "Viagra" and "mortgage," misspellings, strings of numbers in the subject line header, non-Latin character sets, and the like. The exact patterns used vary widely and are in constant flux. Some people in the anti-spam community take the position that the use of certain words is equivalent to sending spam, regardless of the fact that these words have legitimate uses. This can cause problems, and result in wanted mail being junked as spam. EFF has often been a victim of overbroad pattern matching: we have been told that EFF's email newsletter will not be delivered unless we stop using words like "spam," "pornography," and "opt-in." One EFF newsletter was blocked as spam because it referred to a group called "Stop Prisoner Rape." While it's unlikely that EFF's messages are themselves the intended target of anti-spam mechanisms, they are nonetheless blocked due to these imprecise, overreaching techniques.

Spam Assassin, a popular program that does ad hoc pattern matching, assigns "points" to various features of an email to determine whether it is spam. The higher the number of points, the more likely it will be sent to the spam folder or discarded. Points can be assigned for everything from country of origin to certain words or subject headers. One of the major problems with this system is that messages from certain countries – like China, for example – can be blocked purely on the basis of where they come from and what language they're in. The implications for free speech here are very troubling indeed: a human rights group communicating with people in China may find that its bulk email is blocked, and thus anti-spam technology unintentionally works as a political censorship mechanism. Of course, this is only a problem when end users are not given control over how points are assigned and what will be done with messages that get "high" or "low" marks. Spam Assassin and programs like it can be configured to give users more control, and when they are used in this way we recommend them as a solution.

### Collaborative Classification

With this system, users classify documents as spam or not spam, and this classification is sent to a central server. When new lists of classifications are sent to the server, it checks to see whether or not other users have classified the same messages as spam. Thus, a community of people can work together to filter spam. Vipul Ved Prakash's Razor system, as well as Distributed Checksum Clearinghouse (DCC), work this way. Like Spam Assassin, this technique has the advantage that it can be deployed in a way that gives control to end users. The disadvantage is that groups of users may decide to classify an email as spam because they don't like what it has to say. This could result in some people not receiving the mail they desire because the larger group deems it unacceptable.

### Block Lists and White Lists

In this method, some self-appointed authority compiles block lists (and occasionally, white lists) of domain names and/or IP addresses, then publishes the lists on the Internet. Email server operators can subscribe to the block list service and instruct their email servers to deny receipt of email from the listed hosts. This is generally not something the end user

has control over, since a key purpose is to block spam at the SMTP interface, thereby saving bandwidth.

A common form of block list is a list of IP addresses to block, including one or more hosts alleged to have sent spam. The express purpose of this technique is to cause collateral damage, forcibly involving more people in the block list compiler's "cause." Transplanted "offline," this kind of policy would hold that it's reasonable to boycott a store that uses a specific long-distance telephone company simply because the telephone company (not the store) also provides long distance service to someone you dislike. A policy like this is clearly unjust to non-spamming hosts, given that it subjects them to poor treatment simply because they share an ISP with an alleged bad actor.

Occasionally, block lists will block all dynamic and dialup IP ranges, despite the fact that these IP ranges have perfectly legitimate uses. This practice also makes it difficult for tiny non-profit organizations to set up their own mail servers.

In addition, some sites are added to a block list because of the procedures followed by the operators of the email servers at the site; for example, email servers that are configured as open relays (meaning anyone can use them to send email to anyone). The justification for this is that spammers use such servers to hide their identities, despite the fact that open relays have legitimate non-spam uses.

### Email Authentication

Email authentication technologies are intended to help positively identify the server sending a message, and are supposed to cut down on spam messages that "spoof" the identity of sending servers. The idea is to stop people from using fake email addresses to send spam.

Typical systems that enable email authentication include Sender Policy Framework (SPF), SenderID and DomainKeys. These methods enable recipients to confirm that email is from the domain it appears to be from. All three systems share a reliance on augmentations to the Domain Name System (DNS), which links IP addresses to domain names. DNS records have been expanded so that domain owners can identify the specific mail servers authorized to send mail for their domain. When you receive mail purporting to be from Example.net domain, your server might use sender authentication to see if the sending mail server is authorized to send mail from Example.net. Most groups using sender authentication say that if an email fails the authentication test, it is a strong indication that the mail has a forged sender and probably should be blocked.

SPF, SenderID and DomainKeys differ in the specific component of an email message that each tests. SPF (which was recently adopted by AOL) is simplest – it checks the "envelope sender" of an email (which includes the domain name of the mail server initiating an SMTP connection). SenderID delays its checking until after message data are transmitted, and examines several sender-related fields in the headers of an email message to identify the "purported responsible address." DomainKeys checks a header containing a digital signature of the message body and certain parts of the header. This system is more complicated because it verifies the domain of each email sender (the actual "from" address a recipient sees) as well as the integrity of the message.

Many have described the email authentication systems as promoting a policy that says email is "spam unless proven otherwise."

Anti-spam policies based on email authentication can also hinder free speech, as activists participating in online letter-writing campaigns have discovered. The software that enables activist letter-writing campaigns on the net is designed to make it easier for concerned citizens to write email to their representatives about pressing political issues. A concerned citizen writes her letter in an online form and indicates in a checkbox which representative or public official she wishes to reach. The activist campaign software then sends the email on her behalf, putting the letter-writer's email address in the "from" field but sending it from servers at the activist organization providing the service. Unfortunately, emails sent in this fashion appear "spoofed" to email authentication software because the sender's domain is different from the domain where the email originates. One activist reported to the EFF that when she used letter-writing campaign software to tell her senator how she felt about some upcoming legislation, her emails were turned away because he had used SPF email authentication on his server.

## Lack of Due Process

A major issue raised by nearly every spam management scheme is a lack of any kind of process for alerting senders and recipients when their email has been blocked. Companies, organizations and individuals vary widely in their practices in this area.

Sometimes, emails that have been spam-blocked are returned to the sender with a message explaining what has happened.[4] But sometimes, the email is simply deleted and lost forever.

We believe all groups should handle spam blocks in the same way – by using technical standards that already exist. To guide administrators in the creation of computer networks that interoperate with the Internet, the Internet Engineering Task Force (IETF) maintains a list of technical standards documents called Requests for Comments (RFCs).[5] The RFC standard for the outgoing email protocol called SMTP defines a duty to deliver mail or report back on non-delivery.[6] Yet increasingly anti-spam mechanisms and the ISPs that use them are deviating from this requirement in cases of suspected spam. When mail isn't delivered, there is no report back to its source. This is unfortunate, as the RFC serves a real purpose – to keep email flowing and to assist in the detection and correction of errors.

Outside of their duty to adhere to RFC standards, spam blocking organizations and ISPs generally have no specific legal obligation to provide any sort of due process when they choose to block a message, a sender, or an entire IP block. They also have no specific legal obligation to ensure that these blocks are removed when they have been wrongly implemented, or when the spamming ceases. What this means is that when somebody believes her mail is being blocked in error, she has no legal recourse.

Anecdotal reports indicate that some anti-spam services take up to two weeks or longer to remove a sender from a block list. Others report that no process exists at all. Some even claim that anti-spam services are charging senders a fee to be removed from the block list. Obviously these policies create tremendous opportunities for misuse, especially when no objective criteria or requirements for blocking or unblocking exist.

4. Some claim that this is difficult to do on a mass scale. But AOL, one of the nation's largest ISPs, claims that every email they block is accounted for: either its sender is alerted with a bounce notice, or the receiver is told they have received an email which AOL has temporarily classified as spam and placed in a folder which the user can access to be sure it's been appropriately labeled.

5. <http://www.ietf.org/rfc.html>.

6. "The responsibility of an SMTP client is to transfer mail messages to one or more SMTP servers, or report its failure to do so." <http://www.networksorcery.com/enp/rfc/rfc2821.txt section 2.1>.

Delays in getting a sender removed from a block list have a huge impact on political organizations attempting to provide timely information. MoveOn.org uses its list is to give recipients up-to-the-minute information about breaking news and political and cultural events. Recipients rely on the list to do things like help them write their elected representatives before the deadline for a vote on a specific bill before Congress. Since these deadlines are critical as the time for decision approaches, even a slight delay can effectively prevent an email list recipient from making his or her voice heard in the democratic process.

Groups that turn away mail they deem spam should follow the relevant RFC and notify the sender (and, if possible, the receiver) about the block.

## Anti-Competitive, Spiteful, and Politically Motivated Blocking

Anti-spam measures can be misused to silence the speech of groups that the blocking organization or individual does not like. Because it is so difficult to discover and challenge spam blocks, this kind of silencing is pernicious and very hard to control. There are a number of reports suggesting that individuals and groups have been labeled as spammers out of personal malice, anti-competitive behavior, or even fits of pique.

For example, the technology journalist Declan McCullagh reports that SpamCop blacklisted his email list, Politech, evidently because of an alleged spammer's personal vendetta against him. McCullagh had flagged the individual as a spammer by emailing abuse@yahoo.com, so the accused spammer reportedly sought revenge by likewise reporting McCullagh to SpamCop. Without checking on the source of the report, SpamCop listed McCullagh as a spammer. Rectifying the situation proved difficult, and McCullagh was incorrectly listed as a spammer with SpamCop two more times after that.[7]

By implementing the solutions we've outlined in some of the sections above, prejudicial blocking would be easier to catch and stop.

7. See <http://www.politechbot.com/p-03730.html>, <http://www.politechbot.com/p-04121.html>, <http://www.politechbot.com/p-03372.html>.

## Bonded Senders: Barriers to Entry

A growing problem for senders of non-commercial bulk mail is programs designed to stop spam by creating categories of senders who pay to be investigated and designated as non-spammers. The idea is that lists of guaranteed non-spammers can be used to separate out the wheat from the chaff. As a result, bulk mail without a purchased stamp of approval will be more likely to be classified as spam.

A number of ISPs and companies like IronPort and TRUSTe have begun deploying a program like this called Bonded Sender. While details are still being worked out, the basic premise is that only entities or persons who have been "certified" will get their email list messages delivered in a timely or prioritized manner (or, taken to its extreme, delivered at all). Essentially, these programs empower certain entities and organizations to serve as gatekeepers for bulk Internet mail.

These mechanisms are troubling because they could lead to a situation where small players (in terms of funding rather than size of the recipient list) will be unable to use email lists to reach subscribers. Worse, since these mechanisms dock a monetary "bond" whenever the bonded sender companies receive a certain number of spam complaints, they create a situation ripe for manipulation by political enemies or competitors. If someone doesn't like a particular group's message, he or she can report the group as a spammer and actually cost the group money. This wouldn't be a problem except for the fact that most bond programs have no way to check the authenticity of complaints against a given mailer. Moreover, some have acknowledged that they have no formal plans or processes to do so. False or politically-motivated complaints will punish legitimate mailers as if they were spammers.

Another problem with bonded sender programs is that they push email into becoming a "pay-to-play" medium, where people with money can eat their fines and have email delivered on a priority basis, while those with less money face unreliable delivery. While paying to get email prioritized is not a new development online, the bond programs would worsen the problem, perhaps resulting in a world where organizations without financial resources or connections will get their email delivered late or not at all.

If groups participating in pay-to-play programs like Bonded Sender made allowances for non-commercial groups to participate without paying, our concerns would be lessened a great deal.

## Conclusion

Anti-spam measures can and should be deployed as part of email systems. But those who implement these measures must be sensitive to the fact that what they are processing is speech, and that free speech is one of the core elements of a democratic society. If anti-spam measures prevent wanted speech from reaching a willing recipient, whether intentionally or unwittingly, they hurt free speech. If they create additional costs or red tape for groups sending non-commercial bulk email, they damage one of the core benefits of the Internet: the level playing field for speakers.

# Human Rights and Spam: A China Case Study

*Sharon Hom, Executive Director*
*Amy Tai, Internet Project Manager*
*Human Rights in China*
*http://www.hrichina.org*

> *"Regarding Internet security, we use pseudonyms, but the vast majority of Chinese or social classes do not have Internet access. Even though I am [writing] to you, there are thoughts I must keep to myself; there is no opportunity to speak, even briefly, and this is also most regrettable. However, ultimately, one blade of grass can set the prairie ablaze!"*
>
> *--An email received from a Chinese lawyer, who is a reader of Human Rights in China's Chinese weekly e-newsletter, Huaxia Bao.*

Addressing spam email via technology and legislation raises key issues of balancing protection of users from unwanted commercial email while protecting their freedom of expression and access to information. These can be seen in the case of China, a leading source of spam mail, one of the most repressive governments, and a major hub for ICT (information and communication technologies) development, representing particular challenges when implementing anti-spam strategies. Even as the Chinese government signs on rhetorically to emerging international norms and encourages the growth of the Internet, it continues to build a sophisticated architecture of censorship and information control that undermines technology as a tool for empowerment. Actions must be analyzed within the realities of local situations to ensure that the crusade to eliminate spam does not aid governments in the repression of their people. With many ICT companies bidding on projects for the 2008 Beijing Olympics and eager to participate in the China boom, HRIC (Human Rights in China) recommends developing "best" business practices, targeted towards different types of IT (information technology) companies and at multiple levels, integrating an international human rights framework into the development and implementation of anti-spam technology and legislation, and ICT infrastructure at large.

## Technology and Human Rights

Technology has the potential to serve as a tool for empowering peaceful human rights activism and building a more open and democratic civil society through the free flow of information and online collaboration. More specifically the Internet, including email, can be used to amplify dissident and activist voices; generate global support and attention to critical issues; build a virtual space for citizens to meet and organize; and access shared resources inside and outside of China. Such use of technology empowers China's human networks, including Chinese non-governmental organizations (NGOs), workers, peasants, students, religious practitioners, intellectuals, democracy activist, journalists, lawyers, AIDS activists and public health advocates.[1] Technology used in collaboration with human rights activism can advance the development of normative standards that the international community has already adopted, such as freedom of expression and access to information, as articulated in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. In addition to signing and ratifying treaties, many governments are also engaged in global norm-setting processes, such as the World Summit on Information Society (WSIS). The WSIS Declaration of Principles includes equitable distribution and access to technology, and protection of indigenous knowledge, culture, and language, in addition to freedom of expression and access to information.[2]

---

1. Sharon Hom, Amy Tai, and Gabriel Nichols, "The Rise of the Internet and Advancing Human Rights," *China Rights Forum* No. 3, 2004.

2. "Declaration of Principles," World Summit on Information Society, December 12, 2004, <http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160>.

## Disproportionate Development and Information Control in China

Even as the Chinese government signs on rhetorically to emerging international norms of inclusiveness, democracy and a "people-centered" vision of an information society[3] and encourages the growth of the Internet, it continues to build a sophisticated architecture of censorship and information control that undermines technology as a tool for empowerment. The exponential adoption and development of the Internet in China is accompanied by persistent and serious social and economic gaps reflected in a digital divide of gender, economic, geographic and social disparities.[4] In the past seven years, the number of Internet users has grown exponentially from 620,000 to 87 million.[5] The current demographics of Internet users show that 60 per cent of the Chinese Netizen population is made up of young males, and just over half are less than 25 years old.[6] In a country where 364 million young people do not have the opportunity to enroll in secondary education, and where many villages, especially in western China, do not even have sufficient basic infrastructure such as water, power or telephone lines, the potential of the Internet to act as a democratizing force is undermined by uneven access and disparities in economic privilege.[7] As the Human Development Map[8] below shows, along the affluent eastern coast where Beijing, Guangzhou and Shanghai are located, there are significantly higher levels of infrastructure development than in the west, allowing more users to surf the Net from home. Moving away from the financial hubs, a higher percentage of Internet users depend on cyber cafes,[9] which are required by government to use surveillance software

3. "Strengthening cooperation, promoting development and moving towards the information society together," Dec 10, 2003. Statement by H.E. Mr. Wang Xudong, Minister of Information Industry, People's Republic of China at the World Summit on Information Society.

4. Sharon Hom, "The Internet and Free Flow of Information in China," Congressional Executive Commission on China, Apr 15, 2002, <http://www.cecc.gov/pages/roundtables/041502/hom.php> (Aug 4 2004), and Jonathan Watts, "China Admits First Rise in Poverty since 1978," *The Guardian*, Jul 20, 2004, <http://www.guardian.co.uk/china/story/0,7369,1264917,00.html> (Aug 25, 2004).

5. China Internet Network Information Center (CNNIC). <http://www.cnnic.cn> (Aug 4 2004).

6. Id.

7. Asian Development Bank, 2002.

8. China Human Development Index for 2002.

9. Bu Wei, "The Social Impact of the Internet," Presentation at the China Digital Freedom conference at University of Cali-

and are under constant threat of closure by authorities. Thus, official crackdowns on Internet cafes have a disproportionate impact on less economically privileged users and those in the least affluent parts of the country.

In addition to these economic and social disparities, a major challenge to building a more open and democratic China is reflected in the People's Republic of China's (PRC) control over the flow of information. It uses technical, social and legal approaches within a broader existing legal framework of governing state secrets and state security. Firewalls, proxy servers, filtration software for Internet Service Providers and Internet cafes, email and search engine filtration, Web site blocking and surveillance of Internet cafes are among the technical approaches that the Chinese government implements to impede the flow and availability of information to Chinese citizens.[10] In conjunction with filtering, blocking, and surveillance, social methods, such as mass media, ideology and propaganda are used to control the flow of information and social order at large.[11] More than 60 laws govern Internet activities in China, including self-censorship regulations to which over 120 Chinese and international companies have agreed to abide. With over 30,000 state security employees monitoring Web sites, chat rooms, and emails, the PRC executes a very effective police apparatus. Currently, over 60 Internet users are in detention for publishing "subversive" content online, including calling for political reform and the free flow of information.

These technical, social and legal techniques to control freedom of expression and access to information function within a broader, sophisticated and complex framework of national security, state secrets and criminal law. The law defines states secrets as "matters that affect the security and interests of the state…" with information that can be classified retroactively and based on consequences.[12] These methods are not new culturally or historically, but the Internet and new technologies have provided a technological upgrade for the police state. As a result, China's information control has resulted in censorship and self-censorship; a culture and climate of fear; and an undermined capacity to deal with problems.

## Duality Concerns for Anti-Spam Approaches in China

Addressing spam mail via anti-spam technology and legislation raises key issues of balancing protection of users from unwanted commercial email, while protecting their freedom of expression and access to information. Spam, defined as unsolicited commercial email, currently floods 60 per cent of email traffic, posing a significant global problem. Unwanted email presents security and privacy risks, and costs businesses and organizations time and money. To address these problems, governments, multinational corporations, consumer protection groups and others have developed a "cocktail" approach to stemming the flow of spam, using technology, industry best practices, enforcement through legislation, and consumer education measures.[13] The CAN-SPAM Act of 2003 was enacted by the US to regulate spam email, imposing limitations and penalties on violators of the Act. In particular, the Act directs the Federal Trade Commission (FTC) to cooperate with foreign states to minimize the dissemination of unwanted emails.[14]

Information technology and digital communications as tools for empowering human rights activism may be hampered by overbroad anti-spam technology and legislation. The over-breadth and vagueness of the definition and implementation of anti-spam technology may have unintended consequences of blocking freedom of expression. New requirements that email senders identify themselves may undermine protections of anonymity and privacy. The duality[15] of the technology tools raises concerns for a country with an authoritarian government. The tools used to send non-commercial bulk emails, such as domain spoofing and word obscuring, are often deployed by

fornia, Berkeley. May 1, 2004. <http://journalism.berkeley.edu/projects/chinadn/en/archives/002534.html>.

10. Jonathan Zittrain and Benjamin Edelman, "Empirical Analysis of Internet Filtering in China," <http://cyber.law.harvard.edu/filtering/china/> and Open Net Initiative, <http://www.opennetinitiative.net>.

11. Bill Xia, "The Coming Crash of the Matrix," *China Rights Forum* No. 3, 2004.

12. Human Rights in China with China Labour Bulletin, "Labor and State Secrets," *China Rights Forum* No. 3, 2004.

13. J. Trevor Hughes, "The Status of Spam," Presentation at the Spam Consultation at Center for Democracy and Technology, July 15, 2004.

14. CAN-SPAM Act of 2003, <http://www.spamlaws.com/federal/108s877enrolled.pdf>.

15. "Dual use technology" is generally used to define technology that has both military utility and sufficient commercial potential to support a viable industrial base. In this case study, HRIC uses this term to refer to technology that can be used to protect users from spam mail, but also be deployed by repressive governments to control information flow.

activists to avoid detection in face of a government architecture of surveillance and censorship. On the other hand the same email filtering tools that block obscene or commercial content, with nothing more than a change in settings, is used by governments to block "subversive" content. Technological methodology to track down individual spammers can also be used to identify the anonymous author of an email critical of government policies. Legislative solutions should recognize this duality in the use of new technologies. Currently the CAN-SPAM Act includes no explicit safeguards regarding the exchange of information across borders and between governments; this lack of transparency regarding the repercussions of technical assistance to repressive governments is also an issue that arises from the current framework to address spam mail. There is currently no mechanism in place for citizens to monitor the actions of their government under the Act and raise concerns over potential repercussions to freedom of expression or access to information. Time and money spent to protect individuals and non-profits from overbroad anti-spam technology may create higher costs to entry for non-governmental organizations and compromise the democracy-enhancing character of the otherwise inexpensive Internet/email medium.

## Addressing Spam in China

As a leading source of spam email, a country with one of the most repressive governments, and a major hub for ICT development, China raises particular challenges when implementing anti-spam technology and legislation. China sends the highest percentage of spam email in comparison to the amount of "good" email sent.[16] (The US sends between 50 to 55 percent spam email; and close to 60 percent "good" mail.) In defense of China's spam mail problem, the PRC Ministry of Information Industry claims that foreign spammers were utilizing Chinese computers to send spam in order to avoid punishment under their own country's law.[17] As a result, the PRC is asking for more cooperation with other countries in law enforcement to control spam and more assistance from international companies on network security to strengthen anti-spam technology, which raise questions of transparency and the consequences of information sharing across borders.[18]

With the highest number of Internet activists imprisoned[19] and a sophisticated architecture of surveillance and censorship, the PRC is also one of the leading countries in information control.[20] Because anti-spam technology works similarly to filtering and censorship measures that the PRC currently deploys, anti-spam technology and legislation may legitimize China's position to further control and repress the flow of information – both within China, and in and of China. Anti-spam tools may also provide the government with greater ability to track people's actions on the Internet, violating privacy and security rights, and leading to increased self-censorship and more arbitrary arrests and detentions. The intersection of China's state secrets and state security legislation and the over-breadth and vagueness of anti-spam legislation and technology could provide more tools for the PRC government to chill freedom of expression and foster a climate of fear.

## Getting a 'Piece of the Action'

China's booming IT market and its hosting of the 2008 Beijing Olympics are attracting high profile ICT companies to get a "piece of the action." Yet the 2002 self-censorship pledge[21] and recent issues with Google's search engine in China raise questions about the role of companies – both international and domestic – doing work in China. In March 2002, the Internet Society of China asked international and Chinese companies to "volunteer" signing on to a self-censorship pledge, in which companies agreed to refrain from posting information that will "jeopardize state security and disrupt social stability" among other restrictions. A few months ago and still ongo-

16. China sends 15 percent of spam mail and less than 5 percent of good mail. George Webb, "Toward a Spam-Free Future: Microsoft's Anti-spam Vision." Presentation at the Spam Consultation at Center for Democracy and Technology, July 15, 2004.

17. Presentation at ITU on countering spam July 2004.

18. Id.

19. Reporters without Borders, "Internet Under Surveillance," 2004. <http://www.internet.rsf.org>.

20. Out of 167 countries, the Press Freedom Index rated China 162nd, with 167th being the most repressive country of the flow of information. Reporters without Borders. <http://www.rsf.org/article.php3?id_article=11715>.

21. "Public Pledge on Self-Discipline for China Internet Industry," (English translation) <http://www.bobsonwong.com/research/china/selfdiscipline/>. Chinese Version (Internet Society of China): <http://www.isc.org.cn/20020417/ca39030.htm>.

ing, studies by the Open Net Initiative[22] and Dynamic Internet Technology, Inc.[23] on Google's search engine in China show that the Chinese government is filtering search results and keywords. With existing Internet companies already being compromised of filtering their search engines, what are the implications of deploying anti-spam technology in China? How can companies, governments, consumers and NGOs ensure that technology built for China is not also implemented or modified for repressive purposes?

With many ICT companies bidding on projects for the Olympics and eager to participate in the China boom, HRIC recommends developing "best" business practices, targeted towards different types of IT companies and at multiple levels. The circuit tree below describes the path a user request travels, identifying key transactions. Every request routed through the network passes multiple points at which concerns exist for censorship or the invasion of privacy. Starting at the desktop level, Internet cafés and many companies are required to install filtration and surveillance software. At the ISP level it is possible to capture user requests and search for specific terms and data. When the request moves out into the Internet backbone it must pass through the "Great Firewall." Finally, at the destination server information can be collected based both on automated Web logging as well as data requested or offered by the users. Each level is distinct and although the basic concerns stay the same, different mechanisms are needed to protect them based on the technical details of each. Additionally, we have identified examples of some companies carrying the traffic at each level.

Based on the circuit tree below we have outlined a possible framework for exploring best practices that should be developed with the input and participation of multiple stakeholders, including NGOs, consumers, and business. The matrix focuses on three types of IT companies: information providers, hardware and software developers, and connectivity. Mapped to each of type of company are the backbone, Internet Service Provider, and end user levels. The matrix

22. Open Net Initiative, "Google Search & Cache Filtering Behind China's Great Firewall," August 30, 2004. <http://www.opennetinitiative.net/bulletins/006/>.

23. Dynamic Internet Technology, Inc., "Google Chinese News Censorship Demonstrated," September 16, 2004. <http://www.dit-inc.us/report/google200409/google.htm>.

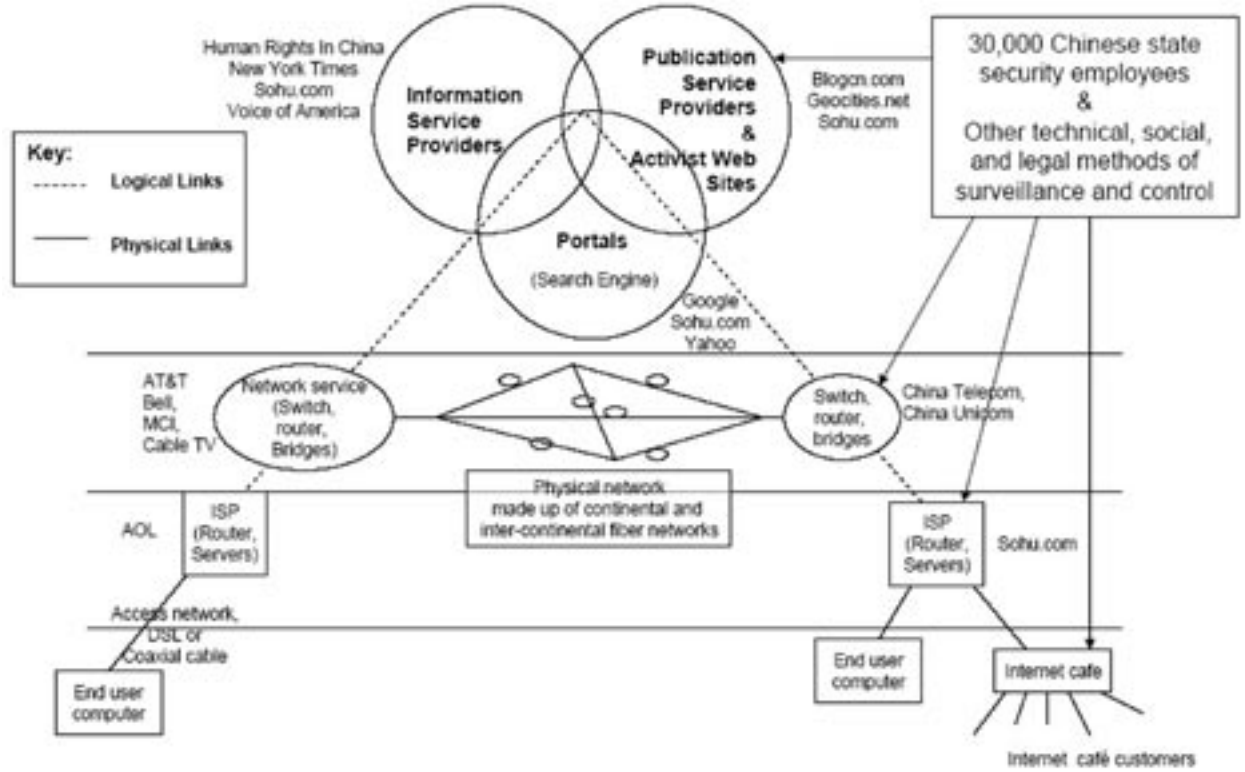


Chart 1: Communication Path
Source: Human Rights in China with contribution from Michael To

reflects a preliminary model for developing best practices that address both domestic implementation and cross-border impact of anti-spam technology and legislation with regards to censorship and freedom of expression; privacy and anonymity; and surveillance and security issues. For each area of concern, the framework identifies some specific issues to consider in developing best practices.

| Types of IT Companies | Examples of Companies Doing Business in China | Levels | | |
|---|---|---|---|---|
| | | End User Issues | Internet Service Provider (ISP) Issues | Backbone Issues |
| Information Providers/ Portals/ Publication Service Providers* | Blogcn.com<br>Geocities.net<br>LexisNexis<br>Sohu.com<br>Sony<br>TimeWarner<br>Yahoo! | (1) Notifying users when information is removed;<br>(2, 3) Retrieving information or posts on public forums without revealing personal identification information | (1) ISP liability for information transmitted over their networks;<br>(2) ISP Record keeping of transmissions over the network;<br>(3) User approval of ISPs sharing information with third parties | |
| Hardware/ Software | Cisco (router, bridge, modem)<br>IBM<br>Microsoft (operating system)<br>Nortel (switch, fiber system)<br>Norton (firewall, anti-virus)<br>Oracle | (1, 2) User Authorization of information transferred via software;<br>(3) Hardware linking unique token numbers to Internet requests/forum posts to specific machines | (1, 2) Retaining individual information on network's users and Web activities in ISP logs;<br>(3) Linkages allowing monitoring of messages sent or received. | (1, 2, 3) Routines that regularly monitor traffic over backbone hardware or software providers' network |
| Connectivity | China Telecom<br>China Unicom<br>MCI<br>AT&T | (2, 3) Monitoring traffic from individual user machines beyond that required to identify network abuse. | | (2, 3) Record keeping and use of logs with any information that would identify the originating machine |

*Recognizing that there is a great deal of overlap with individual companies acting in multiple roles offering different services

**Areas of Concern**
(1) - Censorship/Freedom of Expression
(2) - Privacy and Anonymity
(3) - Surveillance and Security

Chart 2: IT Best Practices Matrix

## Integrating an International Regulatory Framework

China illustrates the dangers of cross-border implementation, on legal, technical, and policy levels, of anti-spam technology and legislation. To address these challenges, HRIC urges policy interventions at multiple levels, integrating an international human rights framework into the development and implementation of anti-spam technology and legislation, and ICT infrastructure at large. An international regulatory framework that can be applied across borders will prevent adverse consequences in other regions. To govern an increasingly global Internet, transparency and accountability for both multinational corporations and governments are critical to properly monitor the modification and implementation of technology. In addition, careful and independent monitoring will ensure that freedom of expression and access to information on the Internet are protected, and that all stakeholders are included in a meaningful way in the design and implementation of the future Internet, both in policy-making and in engineering.