Spam, That Ill O' The ISP:
A Reality Check for Legislators

By Hanah Metchis[1] and Solveig Singleton[2]

Executive Summary

Most public attention has been focused on how spam affects individual email users; less on its impact on ISPs and other administrators of large networks. But the consumer-focused approach is unlikely to solve the most serious aspects of the problem. The consumer is the end of spam's journey; its origins lie in the policies and technologies of networks. Solving most of the problems for ISPs would probably also solve most of the problems for consumers, but the converse is not true. Therefore, this paper assesses spam and its legal and technical solutions with an emphasis on the perspective of ISPs.

We begin by navigating among several competing definitions of spam and outlining its most seriously problematic aspects for consumers, businesses, ISPs, and legitimate marketers. We go on to assess contractual, technical, and statutory solutions.

- For end users, the best solutions are the new Bayesian content filters, which can be tailored to individual preferences.
- ISPs, the most seriously affected, have limited and constrained the spam problem successfully using filters, litigation, and contractual solutions.
- Spammers have been largely forced off of legitimate ISPs onto foreign relays and hijacked ISPs.
- Many (not all) provisions of the new laws proposed thus far are too broad, but none would be helpful without vigorous enforcement.

The study cites empirical research showing that laws have little deterrent effect unless there is a substantial probability that violators will be caught. Increasing the severity of penalties is ineffective if enforcement is ineffective. Many federal and state laws already apply to spam. While a few more carefully targeted laws might be justified, the most effective use of government resources would be increased enforcement at real bad actors.

---

[1] Hanah is a research analyst at the Competitive Enterprise Institute.
[2] Solveig is a lawyer and senior analyst at the Competitive Enterprise Insitute.

Introduction

Spam, which most define as some type or other of unsolicited email, is the issue *du jour*. Everyone agrees it is a problem, but there is little agreement on the best solution. Most public attention has been focused on how spam affects individual email users; less on its impact on ISPs and other administrators of large networks. But the consumer-focused approach is unlikely to solve the most serious aspects of the problem. The consumer is the end of spam's journey; its origins lie in the policies and technologies of networks. Solving most of the problems for ISPs would probably also solve most of the problems for consumers, but the converse is not true. Therefore, this paper assesses spam and its legal and technical solutions with an emphasis on the perspective of ISPs.

We begin by navigating among several competing definitions of spam and outlining its most seriously problematic aspects for consumers, businesses, ISPs, and legitimate marketers. We go on to assess contractual, technical, and statutory solutions. We conclude that while there are some effective technical solutions to help consumers and businesses control spam, ISPs, the most seriously affected, have found only partial solutions. Finally, we conclude effective spam control will come only with innovations in enforcing laws or policies; many (not all) provisions of the new laws proposed thus far are too broad, but none would be helpful without vigorous enforcement. And innovations in law enforcement as always carry their own risks.

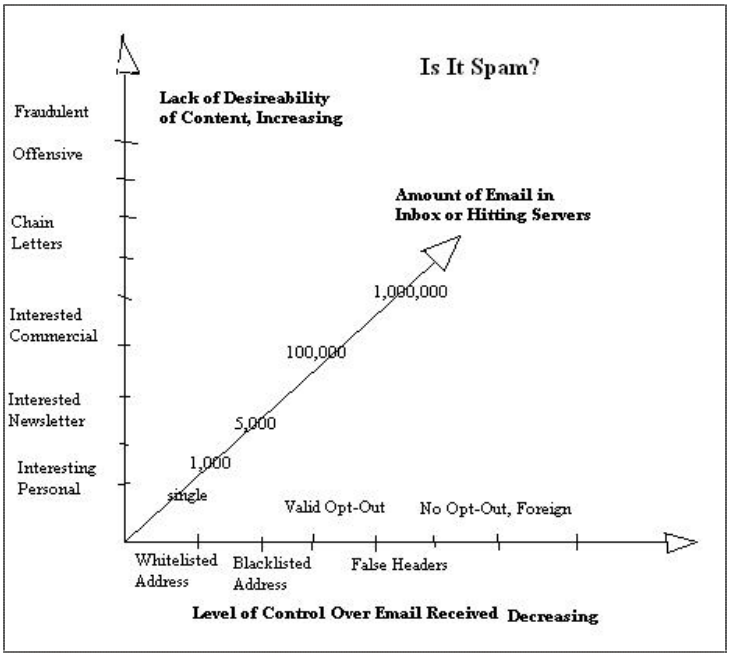
What is Spam?

There are several competing definitions of spam, none of which is entirely satisfactory. One common definition is *unsolicited commercial email* (UCE). This definition excludes unsolicited political messages and some types of fraudulent messages, which most people think of as spam. And it arguably includes such things as résumés sent to potential employers, which are not generally considered spam. Another common definition *unsolicited bulk email* (UBE).[3] This definition is troubling because it suggests that all bulk email should be solicited; but it does not follow necessarily that all unsolicited email is unwanted, or that all bulk email is problematic. Yet another is *unsolicited commercial bulk email* (UCBE). Still others are concerned that the email is *unwanted* or somehow *deceptive* in content or header information.

Picking a single definition for spam is unlikely to point towards good solutions. Every definition highlights an aspect of email that is some people honestly find problematic. And every definition falls short, because it leaves out other problematic emails and often includes emails that are legitimate and wanted by some people. The following graph attempts to capture the complexity of defining spam. The further out any

[3] There is not wide agreement on what constitutes bulk. Some state laws define it (more than 2 messages in Idaho, 500 in Kansas, and 1000 in Louisiana), but most leave the term undefined. Some spammers try to get around such laws, as well as certain types of filters, by including a random string of unique characters in the subject or body of the email, but laws can address this by defining substantially similar emails to be the same.

email is on any one axis, the more likely someone will consider it spam. Note that the y (vertical) axis is subjective—this one is ordered according to one of author's preferences.



Spam, like beauty, is in the eye of the beholder. Some ISPs and anti-spam software makers now define spam as any email the user does not want. This definition is empowering for the end user, since it gives him or her more control over what types of email are blocked. But it is problematic for legitimate marketers and mailing list operators, who lack a concrete set of guidelines for making sure their emails are not spam.

From the standpoint of an ideologically committed privacy advocate, email is problematic if is unsolicited and perhaps if it is commercial. From the standpoint of the real-world consumer, email becomes a problem when it is unwanted, arrives in large quantities, is fraudulent, or contains objectionable content. From the standpoint of an ISP or other large network administrator, it matters mainly when it crashes servers, raises bandwidth bills, and is designed to evade the technological controls that ISPs put in place to block it.

Rather than focus on definitions, therefore, we further dissect spam problems and solutions. Some are probably more worth solving than others, and some require different solutions than others. There will never be a silver bullet for spam. But there are and will continue to be a variety of old standbys and newly developed solutions that solve various portions of spam problems.

The Trouble With Spam

Spam creates a variety of problems for consumers, businesses, ISPs, and legitimate marketers. From unwanted pornographic images to overtaxed servers and

mistakenly blocked emails, these problems are of differing types and severity. A graph can illustrate the complexity of the problem. Solving the spam problem involves untangling the different needs of ISPs, large network administrators, and end users. Some of these needs are technical needs that can be determined objectively but are likely to change rapidly with technology; other needs, such as consumer preferences, also change rapidly – and are subjective and difficult to determine to begin with.

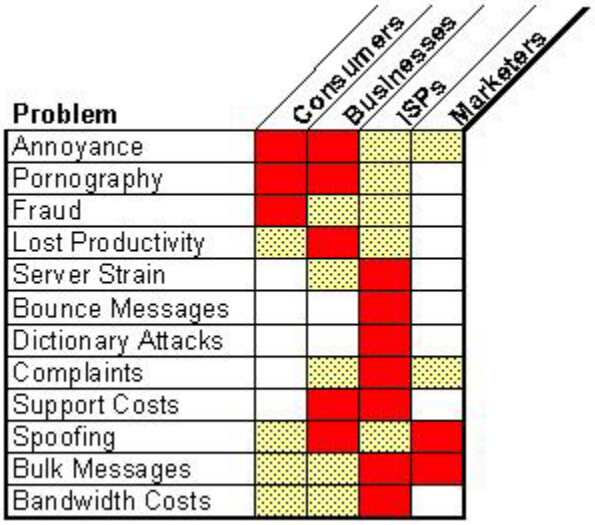


Figure 1: Spam Problems

Red squares indicate a severe problem, yellow a moderate problem.

These problems are growing worse every day, because the amount of spam is constantly rising. Estimates of the amount of spam as a percentage of all email traffic range up to nearly 75%.[4] The amount of spam received by users differs greatly, from none at to hundreds of messages per day for some people.[5] Data from Postini, a spam-blocking filter program that monitors over 1 billion emails per month, shows that the amount of spam is now doubling every five months.[6] America Online America Online gets about 2 billion emails per day. Spam filters installed in 1999 block over 1 billion messages a day. This figure is ten times higher than it was in 1999.[7]

About half of all spam currently appears to come from outside the United States,[8] although many believe that it originates with U.S. residents using foreign relays. This means that even strictly enforced U.S. legislation cannot fully solve the problem. At the

[4] Postini displays real-time percentages of spam in the traffic they monitor at their website, at http://www.postini.com/stats/.

[5] To some extent, users can limit the amount of spam they receive by, to give a few examples, refusing to give out their email addresses, not posting their addresses on websites, using a long address with a combination of letters and numbers, changing email addresses, and never replying to spam.

[6] Postini Email Stat Track (May 2003), at http://www.postini.com/stats/.

[7] Complaint at 2, America Online Inc. v. John Does 1-10, Civil Action 03-474a, April 14, 2003. available at **http://legal.web.aol.com/decisions/dljunk/mexipharmcomplaint.pdf**.

[8] Postini Geographic Origins (May 2003), at http://www.postini.com/stats/maps.html.

rate spam is increasing, if all spam sent from the U.S. was eliminated tomorrow, the problem would be back at today's levels within a few years at most.

Problems for Consumers

Spam is an intrusive nuisance to consumers. It is often described as a privacy problem, but in most cases the spammer knows little or nothing about the consumer. Indeed, this lack of information about the consumer makes the spam problem worse. Millions of emails are sent every day inviting people to enlarge anatomical parts of the opposite gender, lower their mortgage though they live in an apartment, and buy a plethora of products in which they have no interest at all. Parents are particularly concerned about pornographic spam. Spam is also a crime problem for consumers, since a significant amount of spam involves pyramid schemes or other shady ventures.[9]

Several years ago, many ISPs charged their customers for the amount of time they spent online, so downloading and reading spam cost consumers money. Since most ISPs in the U.S. now charge a flat rate, this is no longer a large problem. However, many mobile Internet devices charge users by the hour or minute, so spam could become a cost problem for users once again as these devices become more popular.

Problems for Businesses

Spam costs businesses money in the form of lost worker productivity and the need to upgrade network capacity. According to Ferris Research, spam cost U.S. businesses almost $9 billion in 2002, an amount expected to rise this year.

Technical Support Costs: When hit with certain kinds of spam attacks, businesses have to invest resources in a security investigation. For example, if a spam appears to have been sent from an employee's computer, the company has to check whether that employee has been infected with a virus or spamming-worm, or whether the address was forged by an outside spammer.

Spoofing: Spammers occasionally put the name of a legitimate company in the From header or elsewhere in the e-mail, to give the impression that the message is from the well-known company or is sent with their approval. The reputation of the legitimate company then suffers, since consumers think it is sending out spam. Companies have been successful in suing spammers who do this.[10]

Sexual Harassment: New concerns have arisen with regard to sexual harassment law and its application to pornographic spam. No cases have been brought to court yet, but it is possible that a business could be held responsible for creating a "hostile workplace environment" by not filtering out all pornographic spam. This would create a huge liability for a problem that is not the employer's fault and cannot be reliably solved without a loss in worker productivity due to blocked legitimate emails.

Marketing Difficulties: Spam also affects how legitimate businesses can market their products. Many consumers subscribe to email lists from well-known companies in

[9] A recent study by the Federal Trade Commission found that 66% of spam emails have false claims in the From header, subject line, or text of the message. See *False Claims in Spam*, FTC Division of Marketing Practices, April 30, 2003.

[10] See, for example, *AOL v. LCGM, Inc.* HELP

order to receive special discount offers and notices of sales or new products. However, these emails are sometimes confused with spam messages, either by filtering products or by the recipients. Filters that recognize words common in spam, such as "sale" or "order" sometimes block legitimate, wanted emails as well as spam. In other cases, users forget that they signed up for a mailing list and report the messages they requested as spam, leading to difficulties for the company.

Problems for ISPs

ISPs suffer from spam because it uses large amounts of bandwidth and storage space, but also because it upsets their customers and adds to technical support costs. To combat bulk email, ISPs must build enormous overcapacity into their systems. As the spam problem escalates, some ISPs may find that they are unable to keep up with the rising costs of spam in their systems, and be forced out of business.

Server Strain: Sending or receiving massive amounts of email in a short period of time puts a strain on an ISP's resources.[11] They have to upgrade their equipment and pay higher bandwidth bills to deal with the increase in traffic. Excessive email traffic can severely degrade a server's performance, or even cause it to crash.

Bounce Messages: A significant percentage of the email addresses spammers send to are nonexistent. To avoid the bounced messages, spammers usually put a fake email address in the Reply-To header. Thousands of bounce messages are then sent to another ISP or end user, clogging the servers and costing money for bandwidth.

Dictionary Attacks: Rather than collecting real addresses, some spammers try multiple combinations of common names, or even all combinations of letters, at a popular domain name. For instance, a spammer might send to asmith@aol.com, bsmith@aol.com, etc. This puts a huge drain on the ISP's servers as tens of thousands of e-mails are sent and bounce messages returned for addresses that have never existed.

Customer Complaints: A high percentage of help-desk and customer service time is spent dealing with customer concerns about spam. Large amounts of objectionable email can drive customers away, so ISPs devote lots of resources to blocking spam in order to keep their users happy.

The Root Causes of Spam

Spam is at bottom caused by an economic or pricing problem; ISP pricing structures—pay a flat rate, send and receive all the email you want—disperse the costs of spam onto all users, rather than those actually using bandwidth sending mass emails. And the other costs of becoming a spammer, the software and email address lists, are low. "Fresh" addresses are "harvested" from websites and Usenet posts using automated programs. Software that does this is often bundled with bulk-mailing software. The entire package sells for between $99 and $250. And response rates to spam are good, compared to most bulk snail mail—even though response rates to spam are often less than one tenth

[11] Barry Shein, president of a small Boston-based ISP called The World, notes that some spam contains no legitimate way to contact the seller of the advertised product—websites fail to load, email addresses bounce, and phone numbers are disconnected or never answered. This could indicate that the supposed commercial email is actually a disguised denial of service (DOS) attack aimed at the ISP.

of one percent.[12] In contrast, response rates to opt-in email marketing from companies trusted by the recipient are extremely high compared to even the most successful offline advertising.[13]

Adding to the problem is the lack of a central authority or verification mechanism for email. Decentralized control is one of the things that makes the Internet so powerful, but the structure makes easy and routine verification impossible. This feature cannot be changed without fundamentally altering what the Internet is.

"The" Solution to "The" Spam Problem

The text above shows that there is not just one spam problem, but many, and it is unlikely there will be a single broad solution—unless it's one that sweeps far too broadly and captures a good bit of legitimate email. Unfortunately, most of the wide array of solutions that have been attempted so far are proving insufficient, but they have been partially successful in that spammers have been forced out of some of their early stomping grounds.

Instead of searching for the "one best way" to rid the Internet of spam, consumers, businesses, ISPs, and legislators should address smaller portions of the problem in a variety of different ways. The rest of this paper lays out many of the solutions that are currently in use or have recently been proposed, and explains the benefits and costs of each one. We have divided these plans into three types: contractual, technological, and legal. Some of the "solutions" have the potential to create more problems than they solve, and thus should be avoided. Others show real promise to eliminate some of the problems caused by spam.

Contractual and Cooperative Solutions

If spam is at root a pricing problem, private contracts between ISPs and spammers are the place to start looking for a solution. But because of serious enforcement problems and the general shadiness of spammers, purely contractual and reputational solutions to the problem of spam have limited but not eliminated the problem.

Acceptable Use Policies

Almost all ISP's have strong anti-spam policies that prohibit their customers from sending spam through their servers, both as a netiquette issue and because spam takes up so much bandwidth. Enforcement of these terms has effectively forced spammers to operate through open relays or by hijacking ISPs other than their own.

ISP's' Terms of Service usually also include a prohibition on sending spam to the ISP's customers. However, that provision is universally ignored by spammers. It relies, for effectiveness, on the goodwill of email senders and their willingness to voluntarily follow the rules set out be the ISP. The miniscule number of lawsuits that are filed by ISPs against spammers each year is little deterrent, as we discuss further below.

---

[12] Kosseff, Jeffrey, "Confessions of a Former Spammer," *The Oregonian*, (May 11, 2003), at http://www.oregonlive.com/printer/printer.ssf?/base/business/105256787116000.xml

[13] Opt-in email response rates can be up to 12 times higher than response rates to postal bulk mail campaigns. Cullen, Lisa Takeuchi, "Some More Spam, Please," *Time Magazine*, (November 11, 2002).

Pay-to-send and Pay-to-transmit Models

Consistent with the economic analysis above, since spam happens because it is cheap, in theory, the most effective remedy would be for ISPs, in the ordinary course of business (that is, without litigation), to directly charge spammers for the bandwidth they use. This would cut back on spam across the board the same way that an increase in third-rate postage would reduce direct mailings. But this remedy ultimately that depends on ISPs being able to collect on their accounts payable—and where spammers are involved, that is problematic.

In transmitting an e-mail, the bandwidth of two different ISP's is usually used. The message travels from the sender, to the sender's ISP, to the recipient's ISP, to the recipient. Some ISP's have experimented in the past by quietly making deals with spammers, charging large amounts of money and allowing individual spammers to send bulk emails from their systems. These "pink contracts" generated a great deal of anger in the Internet community, and are now rare in the U.S. Spammers instead bypass their ISP servers by installing their own SMTP servers, or disguise their activities by using open relays in foreign countries or hijacking open proxies run by users with home networks.

The recipient's ISP has a much harder time charging for e-mail, because the source of a spam email is usually hidden. Before a private payment scheme could be put into effect, changes to the email protocol would have to be made. The senders would have to be routinely identified and validated, something which is not built in to current email standards. Note that the price charged to send bulk email to an ISPs customers would have to be steep enough to reduce the amount of bulk email to the point where it was no longer perceived as a nuisance by customers. If a "pay to spam my customers" scheme failed to reduce the amount of spam substantially—close to zero—it would almost certainly raise a huge outcry from users who want to avoid spam altogether. If ISPs are able to identify spam well enough to collect money from its senders, they are able to identify it well enough to block it. Consumers would undoubtedly prefer the latter. The pros and cons of redesigning the email protocol to stop spam are further discussed in the technological solutions section below.

Reputation Effects

The amazing thing is that given the economic incentives, the Internet did not become hopelessly clogged with spam years ago. The reason is probably largely the power of companies' concern for their reputations. Legitimate companies with familiar brand names work hard to preserve the goodwill of their customers. Email from such companies consistently has a valid unsubscribe function, and usually goes out only to customers that have a preexisting relationship with that company or have specifically requested the messages.

Adding to this effect, most consumers realize that companies which use spam usually have some level of shadiness to them. None are established, well-known companies. Some are completely fraudulent. Others appear not to even exist. Many have a tendency to collect some money and then disappear quickly, sometimes setting up again

under a new name. Because of this, most people immediately delete spam, and legitimate companies realize there are better ways to advertise.[14]

Technological Solutions

Software can partially stop the spam problem at several levels. There are many surprisingly efficient tools available for end users to control spam, often provided free of charge. Other blocking techniques can be used by ISPs.

Technology can also aid sender-authentication programs. There are several types of such programs, including e-stamps, bonded sender programs and, more drastically, a redesign of the basic email protocol.

Solutions for Consumers and Business Users

End users mostly just want to keep pornography, fraud, and irrelevancies out of their mailboxes. Some people expect their ISP to solve the problem for them, but such a solution risks blocking what some customers would consider desirable email. User-implemented blocking solutions are likely to produce a better result for consumers in that it is more tailored to their preferences. But this does not help ISPs, as we discuss further below.

Content Filters: These programs attempt to block spam based on the content of the email messages and headers. In the past, these programs were woefully inaccurate, but the newest algorithms, called Bayesean filters, claim to perform with 99% accuracy. They can learn to recognize spam based on the users' classification of emails that are received. Content filters are a lot like guard dogs, in that one must train them and keep close watch on their performance to keep them accurate. Content filters are a great solution for people who can wait a few weeks for full effectiveness, but not the best choice for someone who wants to install a program once and then forget about it.

Whitelists and Challenge-Response: A whitelist is a list of e-mail addresses that are certified as legitimate senders. A user can create a whitelist of everyone in his email address book—friends, family, and the mailing lists he or she subscribes to. Email from all these addresses would be delivered directly to the user with no delays. The question, then, is what to do with mail from people who are not on the whitelist.

In a challenge-response system, the server holds all email from unrecognized addresses while it sends an automated message to the sender of the email. The automated message will verify that the sender is a real person, not an automated bulk email program, by asking him or her to reply to the message or enter some information at a website. If the sender responds appropriately, the original message is sent through to the recipient.

These systems are very effective at eliminating spam, but they create a nuisance for senders that translates into the possibility of missed and delayed mail for the recipient. For instance, a sender might not realize that the automatic message received was a challenge request, and accidentally delete it as spam. Email delivery could also experience long delays when challenges are not immediately seen, for instance if the email was sent as someone was leaving work or going away for the weekend. In addition,

[14] Ibid.

it is a hassle for large legitimate mailing lists, commercial or otherwise, to answer all the challenge messages from new subscribers who have forgotten to add them to their white lists. It could kill the concept of a discussion list, where thousands of people who do not otherwise know each other often communicate together.[15]

While this method might be reasonable for some home users, it's inefficient for businesses, government offices, and individuals who often receive email from people they have never previously contacted.

Collaborative Filtering: Instead of using content heuristics or originating addresses to find spam, some programs use real people. When spam lands in the mailbox of someone who subscribes to a collaborative filtering program, the recipient can report it to the program's server. The server then searches the inboxes of all the other subscribers and deletes all copies of that message. With a large enough subscriber base, most people will see very little spam—it will all be deleted by the time they download their messages.

For quality control, programs can require that a message be identified as spam by two or more people before it is deleted, or they can create "trust ratings" for subscribers based on their past correct identification of spam. But this type of method will always suffer from the fact that different people have different definitions of spam. For people whose email preferences are much different from the norm, collaborative filtering is probably not the best solution.

Collaborative filtering systems also must be able to accurately recognize spam that is unique for each user because of randomized strings of letters, but this problem should be surmountable in advanced systems. For average users who do not mind a few spam emails slipping through now and then, collaborative filtering can be a great way to control the in-box.

Solutions for ISPs and Corporate IT Departments

ISPs and large corporate networks are among the parties hardest hit by the spam problem. They have developed a variety of ways to limit and contain the problem. Though spam is still a large and threatening problem, it would have completely overrun networks many years ago without the blocking techniques currently in use.

Some large ISPs are trying to make it easier for their customers to report and control spam. AOL's most recent versions include a "Report Spam" button in the email display window, which provides the company with more information about spammers, leading eventually to better blocking tools and possible lawsuits. Earthlink is beta testing a challenge-response system that would come bundled with the ISP's software for all users. It is certainly important to make spam-control software easily available to all users, especially novice users who may not be able to find solutions on their own. However, as we have shown, different people need different anti-spam tools to address their particular problems and ways of using the Internet. ISPs that play too active a role risk blocking legitimate messages.

---

[15] TidBITS, an e-newsletter covering the Macintosh community, has published an official policy about challenge-response systems on their website. They refuse to answer challenges sent in response to a mailing list posting, and will answer challenges to individual TidBITS-related emails depending on their workload. "TidBITS Policy on Challenge-Response," at http://db.tidbits.com/getbits.acgi?tbart=07181 (last viewed May 15, 2003).

Blacklist Filtering: Several organizations provide spam blacklists, which collect the IP address information of known spammers. These lists can then be included in filters, to block all incoming e-mail from the blacklisted addresses. While they are extremely effective at blocking spam, they are also quite effective at blocking non-spam.

IP addresses are not always specific to a particular computer or account. Thus, a blocked IP addresses often blocks e-mail from a number of legitimate users, not just from a spammer. Sometimes, entire blocks of IP addresses are added to a blacklist, blocking e-mail from everyone belonging to a certain ISP.

The blacklists are sometimes improperly managed—IP addresses are blocked mistakenly, or because their owners hold opinions that the list managers disagree with. Many blacklists block all IP addresses from specific nations that are notorious for housing spammers. And most blacklists do not publish procedures for being removed from the list, so even if an ISP kicks the spammers off their service, their IP addresses could still remain blocked at the discretion of the list manager. And since the blacklist is activated by the ISP, end users may not even know what is being blocked.

If the problem substantially worsens, we can expect to see more drastic blocking measures taken by ISPs and businesses, such as blocking all foreign relays or suspected spammer-friendly ISPs. Hopefully, such measures would be temporary.

Multi-Party Solutions

Several spam remedies would require collaboration between ISPs, bulk mailers, and consumers to be effective. Others could only be enacted through a redesign of the basic email protocol (SMTP), making current email programs obsolete. Though they would be difficult to implement, some of these proposals promise much better solutions to the spam problem than more easily available technologies.

E-Stamps and Bonded Sender Program: These two methods let legitimate senders take responsibility for their emails. For e-stamps, the sender pledges a certain amount of money per message that will be paid if the message is reported as spam. For a bonded sender program, the sender deposits a sum of money with a bonding company per mailing. These pledges are noted in the headers of the emails to ensure that they are not be blocked by ISPs. If a recipient decides that the message is spam, he or she reports the abuse either by pressing a “this is spam” button or by some other program-specific method. The money is then collected by the recipient’s ISP.

Such a program would require a great deal of coordination between e-stamp and bonding companies as central authorities and ISPs as program participants. If the ISPs do not recognize the stamp or bond, the email could be blocked despite the pledge. If they do not provide an easy way for their users to report abuses, spammers using the program might escape with little or no penalty.

E-stamp programs are usually intended to be used by all email senders, including ordinary, non-bulk senders. This could create a great deal of abuse, since the recipient is given the final authority to decide whether a message is spam and money should be collected from the sender. Estranged lovers and annoyed acquaintances could report messages that are clearly not spam, costing innocent people a significant amount of money.

Bonded sender programs, on the other hand, are intended only for bulk mailers. But many legitimate bulk mailers cannot afford to post bond for their messages. Non-profit institutions and hobbyist newsletters are frequently run on small budgets, and the risk of getting fined by political opponents or forgetful new members could make them think twice about communicating through email.

Protocol Redesign: A secure protocol for sending email, perhaps based on security certificates, would make it easier to identify the sender of an email. It would be a secure, verified protocol, something like HTTPS. The current protocol could still be used, but end users in their email client or ISPs at the server level might choose to accept only messages sent with the secure protocol.

Under a secure protocol, anyone sending spam would be immediately identifiable, and then could be effectively prosecuted under anti-spam laws. Spammers might still choose to send e-mail using the unsecured protocol, so as to remain anonymous, but they might then find that their messages are bounced by most people because most people will only accept the secure protocol. This approach could be combined with a whitelist, so that known friends could be permitted to use the unsecured protocol, but unknown senders would have to use secure identity verification.

There are some concerns that sophisticated spammers could hack a verification system and send their messages anyway, but any proposed system would have to be evaluated against this individually, so we can offer no general recommendation here. But it is quite important to understand that verified email has the potential to change the spirit of the Internet. Easy communication between any two people, without centralized authorities as watchdogs, is a fundamental Internet value. Changing this may bring benefits, but should not be done lightly.

Legal Solutions

As of this writing, about 29 states have passed laws against spam.[16] Several federal bills are pending.[17] Federal trademark law and the Computer Fraud and Abuse Act presently have been used against spammers, so the common assertion that the United States has no federal spam law is not quite true. But the medley of state and federal laws available so far are almost completely ineffective at deterring spam, although they do allow some individual spammers to be sued. Litigation is just not the most effective way to shift costs onto spammers. In addition to being difficult to trace because of the use of fake headers, many spammers are out of state and/or use relays based in other countries, and the number of foreign spammers will almost certainly grow over the next several decades as more people come online in other nations. Presently, Asians are leading the pack.

Setting the enforcement problem aside for the moment, many of the anti-spam laws that have been proposed are inappropriate because they criminalize legitimate

[16] For a regularly updated list and summaries of state laws, see Professor David Sorkin's web site, "Spam Laws," at http://www.spamlaws.com.
[17] For an updated guide to federal bills, see Ibid.

communications or technology. There are, however, exceptions—legislation that targets fraudulent or destructive conduct. The section below sorts this targeted legislation from the overbroad or useless. We start with the better laws and move to the bad ones.

Falsified Header Info

Most states have made it illegal to falsify or forge header information. This needs careful definition, since many ordinary users change their Reply-To information for legitimate purposes. (For instance, using a web service to check e-mail while on vacation but wanting people to reply to your main address.) Two federal bills, the CAN-SPAM Act of 2003 (S. 877) and the REDUCE Spam Act of 2003 (H.R. 1933), restrict falsified headers in unsolicited commercial email.

The outlawing of falsified header information makes a certain amount of sense. It is a form of fraud. If it would be a fraud or trespass for someone to misidentify themselves to obtain entrance to a building in order to propose a face-to-face commercial transaction; it makes a certain amount of sense that a mechanical misidentification is also a fraud. The network protocols are merely stand-ins for human actors. Being able to deal with this kind of fraud is likely to be increasingly important as more and more transactions take place between machines instead of people.

The right to speak anonymously, which has a long pedigree in American constitutional law and human rights practice, could be a constitutional problem with a law against false header information.[18] Fundamentally, a law requiring accurate header information is a requirement that in order to speak, one must identify oneself. Arguably, though, a spammer who violates an ISP's terms of service policy by sending damaging amounts of bulk email and uses a fake header to do so is acting well beyond his rights, in that he is in breach of contract and possibly trespassing as well.

A law that banned falsified, forged, or concealed header information would almost certainly be unconstitutional—or, outside the U.S., just plain unjust—if applied to those sending *individual* (as opposed to bulk) emails with forged addresses. However, a properly crafted law could require accurate headers in some cases. There is a distinction between outlawing a message because of its content (false identification) and outlawing a message or series of messages that causes damage to property. Publishing an anonymous essay is protected, but dumping a huge stack of anonymous pamphlets on someone's lawn is not.

A prime example of faked or concealed headers that should be protected is email sent by political dissidents. Making certain that the laws exempts individual use of anonymous remailers or anonymizing software would be important.[19]

---

[18] Technical changes to the network itself to authenticate email senders do not raise constitutional concerns because there is no state action, assuming private network builders undertake these changes voluntarily.

[19] As a technical matter, most anonymous remailers are set up so that only one message at a time may be sent through them, making them impractical for use by spammers; each message sent though a remailer also instructs the recipient on who to contact in case of abuse. <http://www.technomom.com/writing/anonheaders.html> And they tend to be closely monitored and enforce anti-spam policies as well. <See, e.g., http://www.anon-remailer.gq.nu/anon_remailer.htm>

None of this means that a law against falsified or forged headers would be easy to enforce; the state laws have not proved so. But such a law could be crafted so that most enforcement actions would not be unjust or overbroad.

Focus on Damage

Nevada has an interesting element to its anti-spam law, making it illegal to send emails with falsified routing information that are reasonably likely to disrupt the normal operation of a computer, web site, or email address. This gets around the difficulty of defining spam by going straight to the question of whether the spammers are actually hurting the ISP or end user. For some reason, other states have not followed this course. And there seem to have been no cases brought under this aspect of the Nevada law (or indeed any aspect of the Nevada anti-spam law).

Civil Lawsuits & Common Law Remedies

ISPs, individuals, and businesses damaged by spam have sued spammers on a wide variety of grounds—federal statutes, state statutes, and common law. Falsified headers lead to claims based on trademark infringement on the part of hijacked ISPs or business sites.[20] Another significant category of suits is based on common-law claims such as trespass[21] to chattels,[22] unjust enrichment or misappropriation,[23] or unfair competition. The Federal Computer Fraud and Abuse Act, 18 U.S.C. section 1030 (a) is also commonly invoked with success.

Out of all this litigation, some lessons stand out: Even the most well-funded and vigorous plaintiffs, such as AOL,[24] have encountered increasing spam loads in spite of having brought multiple successful lawsuits. Spammers against whom a successful suit has been brought once may have to be sued again for ignoring the terms of a previous settlement or injunction.[25] It took several *successful* lawsuits over two years from well-funded and persistent plaintiffs to shut down one of the most visible and notorious spammers, Cyber Promotions. And money judgments against spammers are hard to collect.

Some have advocated "bounties" to encourage consumers to sue spammers. This might be helpful, but it is doubtful that a significant number of consumers will participate in this scheme. The damage that any individual spammer does to any individual consumer is slight; judgments are hard to collect, and the time that must be invested is considerable. There might be some potential for the plaintiff's bar to pursue class actions

---

[20] See, e.g. Cyber Promotions, Inc. v. America Online, Inc., 948 F.Supp. 436 (E.D. Pa 1996) (AOL brings trademark claim)(Cyber Promotions actually sued AOL in this early case after AOL retaliated against the spammer with an "email bomb"); America Online, Inc. v. LCGM Inc., 46 F. Supp 2d 444 (E. D. Va. 1998)(trademark and other claims).

[21] See, e.g. AOL Inc. v Prime Data Systems, 1998 U.S. Dist. LEXIS 20226 (1998)(Trespass to chattels case in which AOL showed costs of .00078 per email message sent, not counting personnel time).

[22] CompuServe, Inc. v. Cyber Promotions, 962 F. Supp. 1015 (S. D. Ohio 1997).

[23] Earthlink Networks v. Cyber Promotions, Case No. BC167502 (Calif. Super. Ct. May 7, 1997).

[24] See documents from America Online's suits at http://legal.web.aol.com/decisions/dljunk/index.html

[25] Earthlink initially won an injunction against Cyber Promotions, but had to go back to court a year later when the defendant violated it. In the later case, Earthlink won a two-million-dollar judgement credited with putting Cyber Promotions out of business.

against spammers, but for one problem: most spammers are not "deep pockets," and plaintiff's attorneys generally want to be paid. And so they may well seek to blame someone for spam other than the spammers. One attorney, for example, advocates suing the United States Government for spam.[26] More logical and sometimes wealthy targets are the ISPs themselves. This might make some lawyers rich but is unlikely to do anything to stop actual spammers.

Finally, like many of the anti-spam statutes we review below, some of the common-law anti-spam precedents are disturbingly broad in their consequences. Law professor Dan Burk has written an excellent article exploring the implications of ruling that the transmission of electrons can be a form of trespass to chattels.[27] Electrons are everywhere; if they can trespass, he points out, we are going to have trouble keeping track of all the potential trespasses we can commit. Disturbingly, Ebay later used a trespass to chattels claim to shut down a potential competitor from using bots to explore their site.[28]

Labeling

Many states require spam to have *[ADV:]*, *[advertisement]*, or *[ADV:ADLT]* at the beginning of the subject line. The purpose of such a law is to aid filtering and manual deletion. However, depending on the definition of spam in these bills, the rules might also apply to legitimate marketers, which would actually make filtering more difficult. And this type of legislation does nothing to stop ISP's problems and actually might make them worse—millions and millions of messages would and could continue to pound away at the servers, immunized from liability by a label.[29] H.R. 1933 and S. 877 both contain labeling requirements for unsolicited commercial email messages, the limits in H.R. 1933 being restricted to bulk messages.

Mandatory Unsubscribe or Working Opt-out Requirements

Many state laws require unsolicited email to include working instructions for being removed from the list. This has the same potential problem as labeling, allowing spammers to pound away at servers all they like so long as they include opt-out instructions. Since spamming companies are so often temporary, being removed from one company's list means next to nothing. As we note above, legitimate companies already regularly include valid unsubscribe links.

A related type of law would establish a "do not email" list administered by the Federal Trade Commission. The usual criticism made of this law is that it would be used by spammers to spam those on the list. Supposing (unrealistically) that it would not be, it would be overbroad and bar many potentially desirable email contacts.

---

[26] Jonathan Bick, "Spam-Related Class Actions are on the Horizon and the U. S. Government Could End Up as a Defendant," New Jersey Law Journal Vol. CLXXII No. 5, Index 341, May 5, 2003.

[27] Dan L. Burk, "The Trouble with Trespass," Journal of Small and Emerging Business Law, Spring, 2000.
[28] Jay Hollander, "Raising the E-Drawbridge on Cybertrespass," New York Law Journal Vol. 228, November 26, 2002.

[29] Eric Hall, A Call to Arms, http://www.ehsco.com/opinion/19971117.html

Restrictions on Email Harvesting or List Sharing

Some people have proposed restricting the harvesting of email addresses from web sites. Assuming meaningful enforcement, is this approach appropriate? In principal, it does not seem right to outlaw the mere *collection* of information from web sites. It is conceivable that address harvesters could be used carefully enough and only to send highly targeted email to people likely to want it, in which case it might neither harm servers nor be perceived as a nuisance. Adding another component to such laws, so that they punish collecting plus some overtly harmful action, would be better. If website administrators want to keep harvesting bots off their websites, there are technical tricks they can employ.[30]

Other laws and proposals, such as the "Bradstreet Bill" in Michigan, are intended to prohibit trade in email lists between ISPs. In fact, the Michigan bill was so poorly drafted that it in effect *outlawed email itself.* This is because every time an ISP carries an email for a customer to another ISP, it is "transferring" the customer's email address to the other ISP in violation of the law. Legitimate ISPs are unlikely to trade email addresses to spammers in any case. In short, restrictions on harvesting or gathering email addresses are overly broad.

Opt-In

Opt-in is widely supported by anti-spam activists who support legislation as a good legislated solution to spam problems. Again assuming that the law can be effectively enforced, however, opt-in laws would restrict and punish a good deal of behavior that is neither wrong nor problematic. It is bizarre to think that one should be permitted to send email only to those from which one has had an explicit invitation. Unsolicited and unwanted are not necessarily the same thing, even for commercial email. *Untargeted* and unwanted are more likely to coincide. For example, one of the authors has been searching fruitlessly for some time for the following products: A hobby-sized table saw with a dado blade; women's cuff links; and a "winking kitty" T-shirt glimpsed on the character "Willow" in *Buffy the Vampire Slayer*.[31] Should some entrepreneur process her desperate google and ebay searches for any of these products and send her an unsolicited email explaining how she could obtain them, she would fall out of her chair with joy. For another example of an unsolicited, targeted email that was very much wanted, see Appendix B.

The adherence to opt-in among activists may be best explained by a theoretical conviction that people have a right to control information about themselves. This makes sense for medical information and some other types of very personal information, but not for names, addresses, phone numbers, and much ordinary shopping behavior. Opt-in is a broad radical departure from our tradition of the freedom of information. The general rule in the United States has been that ordinary people, journalists, and businesses have been free to learn about other human beings without asking their permission, with some narrow exceptions.

---

[30] http://hacks.oreilly.com/pub/h/221

[31] The "winking kitty" tee can be viewed at the award-winning web site "Yummy Sushi Pajamas," at http://www.laurelleaves.com/YSP/fun7.gif.

Many highly visible businesses voluntarily use opt-in for emailing prior customers. It is a viable option for large companies with familiar brand names and a nationwide reputation and catalog mailing list, since consumers with an interest in their products already know about them and are likely to visit at some point. But for small ventures, niche ventures, and start-ups, mandatory opt-in is likely to preclude their using email as a marketing medium at all, even with careful targeting and responsible bandwidth usage. The representative of one small company said the following about their email newsletter, which they send out every other month to announce new products and sales:

> We don't consider this SPAM but under newly proposed regulations there is the danger that it could be interpreted that way. The letter usually generates a spike in repeat business for us that lasts about a week. The sale spike makes all the difference for us because it usually makes that month a profitable one. We use an Opt in e-mail list as well as including all new customers who buy anything from us. Of course, anyone can opt out. Each month we usually get at least one of the recipients responding back with bitter acrimony about being spammed. They forget that they opted in for the e-mail list. There is the danger that one of these recipients could cause a lot of problems for us under any new regulations.[32]

And mandatory opt-in, with its risks of litigation and attendant legal risks and costs is likely to cause problems even for large businesses. Meaningful enforcement of a far less overbroad law would better target real "bad actors."

Technology Bans

A few states, including Illinois, Kansas, Louisiana, Nevada, outlaw "spamware" —bulk mail software, e-mail address harvesters, and programs that falsify headers. This represents another overbroad approach. Many legitimate email programs and powerful software like Unix allows users to perform the same functions as spamware.

Enforcement Problems

Throughout the discussion of statutes above, we have assumed that the laws would be enforced at some reasonable level. In fact, this is a wholly unrealistic assumption. Spam prosecutions have not been a priority for state prosecutors, and there is no reason to suppose they would be a priority for federal prosecutors. Individual states' long-arm jurisdiction can extend to out-of-state spammers, though perhaps this is unwise. In response to a federal law, many spammers are likely to begin to shift operations overseas.

Spammers are difficult but not usually impossible to trace. But even when they are identified, bringing a lawsuit is time-consuming and expensive. Often, spammers have disobeyed court orders, and judgments against them are rarely collected. Offering a bounty to private parties to bring suit against spammers might help, but few private parties will relish being entangled with the legal system even for a few thousand dollars.

---

[32]Email from Jim Santo to Braden Cox, on file with author, May 3, 2003.

Still, commentators continue to talk as if a federal anti-spam law will solve the enforcement problem or will deter spam simply by threatening harsher punishments. This is not so. Empirical research on deterrence has shown again and again that the deterrent effect of a law depends mainly on how likely the offender is to be caught. A law that threatens a steep punishment but is rarely enforced will have almost no deterrent effect; laws against drugs are a case in point.[33] However, a law that threatens a very mild punishment will have a deterrent effect if there is a high probability that the offender will be caught.[34] The fact that spam persists in spite of state laws against it suggest strongly that the spammers simply do not care that their conduct is illegal. Enforcement being rare, they have little reason to worry. A few token large cases are not nearly enough.

Spam is therefore part of a larger problem with electronic commerce: how to enforce laws across jurisdictional boundaries. Some have celebrated the freedom from national laws that the Internet offers, perhaps not realizing that the lack of accountability enables fraud as well as free speech. On the other hand, the network and its users may have more power to absorb and adapt to abuses than we all anticipate—recall the dire predictions of the mid 1990's that the Internet was on the verge of collapse.

The main point, however, is that the spam problem is exacerbated by lack of enforcement. This is where resources should be directed—not only to think out new methods for fairly enforcing essential online norms, but whether new procedural or substantive standards of due process are necessary to protect civil liberties.

---

[33] Empirical evidence shows that increasingly severe punishments is a less effective deterrent than increasing the probability the violator will be caught. See CRIMINAL LAW AND ITS PROCESSES 117 (Sanford H. Kadish & Stephen J. Schulhofer, eds., 6th ed. 1995).

[34] Studies of individual-level tax compliance have also found that the severity of the penalty is less of a deterrent than the probability of detection. Dick J. Hessing et al., Does Deterrence Deter? Measuring the Effect of Deterrence on Tax Compliance in Field Studies and Experimental Studies, in Why People Pay Taxes: Tax Compliance and Enforcement 291-92 (Joel Slemrod ed., 1992); see also Brian Erard, The Influence of Tax Audits on Reporting Behavior, in Why People Pay Taxes, at 95, 113-14. These studies suggest that the weight of a sanction on ly becomes relevant after the likelihood of being caught becomes substantial.

Appendix A: Anti-Spam Products

The following is not an exhaustive list of anti-spam products, nor are the products endorsed by the authors. This list is included only to show the wide variety of products that are attempting to address the problems caused by spam in a number of different ways. Some of the products listed are only available for certain platforms or email programs.

Many of the programs in this list combine more than one spam filtering method. We have included them under the main feature they use.

For Consumers

Bayesian Content Filters:

- POPFile - http://popfile.sourceforge.net/
- Bogofilter - http://sourceforge.net/projects/bogofilter
- Outlook Spam Filter - http://www.outlook-spam-filter.com/

Challenge-Response:

- Matador - http://www.matador.com/products_matador.html
- Mailblocks - http://about.mailblocks.com/index.html
- SpamArrest - http://spamarrest.com/

Collaborative Filtering:

- SpamNet - http://www.cloudmark.com/products/spamnet/

For Businesses and ISPs

- Postini - http://www.postini.com/
- Brightmail - http://www.brightmail.com/
- Spamhaus Blacklist - http://www.spamhaus.org/index.lasso
- MAPS RBL Blacklist - http://mail-abuse.org

Multi-Party Solutions

- IronPort Bonded Sender Program - http://www.bondedsender.com/

Appendix B

Example of Desired, Yet Unsolicited Email Sent to One Author

Below is an excellent example of the kind of unsolicited mail that might be made illegal under a spam law, but that one author considered legitimate and very much wanted. The email came from a site the author regularly visits but has never given her information to. It was, however, well-targeted: they know the author has a blog and am interested in conservative commentary. The recipient was quite interested in their service, and signed up immediately. This is unsolicited and arguably commercial (they don't want me to buy anything right now, but they are advertiser-supported and will make money from more people reading their site), and bulk. But it's wanted (at least by some), non-fraudulent, and targeted.

TO: Online Publisher

FROM: [individual name omitted]

RE: Opinion Alert - Conservative Commentary in your inbox

I would like to take this opportunity to bring to your attention Townhall.com's free flagship product, the Opinion Alert.

I've included today's edition so you can see for yourself what it looks like.

Six days a week over 100,000 subscribers receive the most comprehensive conservative op-ed page in the world from Townhall.com. Over 65 columnists contribute dozens of columns each week and Townhall.com puts them all in one convenient place for you.

Just after midnight each day, a dozen or more of the best commentaries around are delivered to your inbox. You can read one, two or all of the day's articles if you like. Link to them if you think your readers will enjoy them.

With the Townhall.com's Opinion Alert you'll have writers like George Will, Ann Coulter, Thomas Sowell, David Horowitz, Jonah Goldberg, William F. Buckley and many more at your fingertips. The full list is available at http://www.townhall.com/columnists/ Townhall.com is a completely free service and so is the Opinion Alert.

I would like to send you this terrific service for free. If you agree that the Opinion Alert is something you've been looking for, you can subscribe quickly here:

Tuesday, May 13, 2003

Time to pressure Iran
by Peter Brookes (5/13)
With so much attention focused on Iraq and North Korea lately, it's not surprising that we've been hearing little about the other member of the Axis of Evil. The irony is that, in many ways, Iran is worse than the other two.

'Transformation, part deux'
by Frank J. Gaffney, Jr. (5/13)
By appointing Donald Rumsfeld and his team to run the Pentagon, President Bush found people with the vision, courage and tenacity needed to make the policy and hardware choices that will do much to determine whether the armed forces will be as effective in contending with future threats to the Nation's security as they were recently shown to be in liberating Afghanistan and Iraq.

The deficit is big enough to take care of itself
by Rich Lowry (5/13)
President Clinton would like to claim that his 1993 budget plan erased the deficit. Republicans would like to claim that their kamikaze anti-spending charge in 1995-'96 did it. In fact, both parties were largely spectators as economic growth trampled the deficit for them.

Should illegal aliens get driver's licenses?
by Phyllis Schlafly (5/13)
The hottest controversy in state legislatures today regards allowing illegal aliens to obtain driver's licenses. Americans were shocked to discover that most of the 19 hijackers on 9/11 carried driver's licenses from Virginia, Florida or New Jersey.

Republicans announce new initiatives
by Armstrong Williams (5/13)
House Speaker Dennis Hastert and Senate Majority Leader Bill Frist pledged last week to "fulfill America's Promise," by signing a series of initiatives geared toward empowering black Americans.

Toning down whose rhetoric
by Cal Thomas (5/13)
The National Association of Evangelicals (NAE) convened a meeting in Washington last week to urge their mostly conservative Christian leaders to tone down "dangerous" and "unhelpful" remarks about Islam.

Shooting the economic wounded
by Doug Bandow (5/13)
America's series of corporate scandals have demonstrated the power of the market to discipline errant businesses. Market forces can also rehabilitate firms, unless Uncle Sam decides to shoot the economy's wounded.

The President gets it
by Jack Kemp (5/13)
In reading the president's speech, it dawned on me how well he understands the necessity not only of laying out a road map to peace between Israel and the Palestinians but also of paving that road to peace with sound economic policies for

the entire region so as, in his words, "to bring the Middle East into an expanding circle of opportunity, to provide hope for the people who live in that region."

About those COPS
by Mona Charen (5/13)
Remember Bill Clinton? Before life got serious, Bill Clinton used to work incredibly, just amazingly hard fixing the problems that plagued America.

They know the stakes, all right
by Bill Murchison (5/13)
A word needs to be said in praise -- yes, I said praise -- of the Democratic senators now blockading the confirmation of judicial nominees Miguel Estrada and Priscilla Owen.

Inside the numbers: The prom
by Matt Towery (5/13)
Over the past weeks, television news superstar Bill O'Reilly and other respected journalists have focused their disgruntled attention on an "all-white" private party held in Georgia's small and predominantly rural Taylor County.

My week at Stanford
by Dennis Prager (5/13)
I spent last week at college. And not just any college. Stanford University.

Exit ignorant
by Debra Saunders (5/13)
State Board of Education member Suzanne Tacheny has heard students wail that the requirement to pass the state's high school exit exam could ruin their chances of getting into college. They are so wrong, she said.

Conservative News and Information at www.townhall.com

Sincerely,

[individual's name omitted]