

SPAM AND ITS EFFECTS ON SMALL BUSINESS

HEARING

BEFORE THE

SUBCOMMITTEE ON REGULATORY REFORM AND
OVERSIGHT

OF THE

COMMITTEE ON SMALL BUSINESS
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

WASHINGTON, DC, OCTOBER 30, 2003

Serial No. 108-44

Printed for the use of the Committee on Small Business



Available via the World Wide Web: <http://www.access.gpo.gov/congress/house>

U.S. GOVERNMENT PRINTING OFFICE

93-042 PDF

WASHINGTON : 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON SMALL BUSINESS

DONALD A. MANZULLO, Illinois, *Chairman*

ROSCOE BARTLETT, Maryland, <i>Vice Chairman</i>	NYDIA VELÁZQUEZ, New York
SUE KELLY, New York	JUANITA MILLENDER-McDONALD, California
STEVE CHABOT, Ohio	TOM UDALL, New Mexico
PATRICK J. TOOMEY, Pennsylvania	FRANK BALLANCE, North Carolina
JIM DEMINT, South Carolina	DONNA CHRISTENSEN, Virgin Islands
SAM GRAVES, Missouri	DANNY DAVIS, Illinois
EDWARD SCHROCK, Virginia	CHARLES GONZALEZ, Texas
TODD AKIN, Missouri	GRACE NAPOLITANO, California
SHELLEY MOORE CAPITO, West Virginia	ANÍBAL ACEVEDO-VILA, Puerto Rico
BILL SHUSTER, Pennsylvania	ED CASE, Hawaii
MARILYN MUSGRAVE, Colorado	MADELEINE BORDALLO, Guam
TRENT FRANKS, Arizona	DENISE MAJETTE, Georgia
JIM GERLACH, Pennsylvania	JIM MARSHALL, Georgia
JEB BRADLEY, New Hampshire	MICHAEL MICHAUD, Maine
BOB BEAUPREZ, Colorado	LINDA SANCHEZ, California
CHRIS CHOCOLA, Indiana	ENI FALEOMAVAEGA, American Samoa
STEVE KING, Iowa	BRAD MILLER, North Carolina
THADDEUS McCOTTER, Michigan	

J. MATTHEW SZYMANSKI, *Chief of Staff and Chief Counsel*

PHIL ESKELAND, *Policy Director*

MICHAEL DAY, *Minority Staff Director*

CONTENTS

WITNESSES

	Page
Beales, Hon. J. Howard, III, Federal Trade Commission	3
Cerasale, Jerry, The Direct Marketing Association	8
Goldberg, Bruce, Weatherman Records	10
Rizzi, John A., e-Dialog, Inc	12
Giordano, Catherine, Women Impacting Public Policy	15
Ham, Shane, Progressive Policy Institute	17
Crews, Clyde Wayne, Jr., Cato Institute	20

APPENDIX

Opening statements:	
Schrock, Hon. Ed	33
Prepared statements:	
Beales, Hon. J. Howard, III	35
Cerasale, Jerry	53
Goldberg, Bruce	59
Rizzi, John A.	61
Giordano, Catherine	74
Ham, Shane	80
Crews, Clyde Wayne, Jr.	85

HEARING ON SPAM AND ITS EFFECTS ON SMALL BUSINESS

THURSDAY, OCTOBER 30, 2003

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SMALL BUSINESS,
SUBCOMMITTEE ON REGULATORY REFORM AND OVERSIGHT,
Washington, D.C.

The Subcommittee met, pursuant to call, at 10:33 a.m. in Room 2360, Rayburn House Office Building, Hon. Ed Schrock [chairman of the Subcommittee] presiding.

Present: Representatives Schrock and Gonzalez.

Chairman SCHROCK. Good morning, everyone. I think we will go ahead and get started. I am sure other Members will come in. Rumor is we are supposed to have three votes at 10:30, but you know how that goes around here. It may be a little bit after that. I will go ahead and do my opening remarks. We will let Mr. Beales do his, and then we may have to go vote.

Since inception of the Internet and electronic mail, businesses have found opportunities to use both as vehicles of marketing and advertising. Every day, Americans receive billions of e-mails, and its low cost allows marketers and business people to reach wider audiences than ever before.

Unfortunately, like any business practice in the United States, there are those who abuse this technology by sending bulk, unsolicited e-mails to users without their permission. Spam, as it has been dubbed, is estimated to constitute over 40 percent of commercial e-mail. It clogs e-mail servers, reduces productivity, inhibits growth and has a direct affect on small businesses in the U.S.

There are, however, many small businesses in the United States who execute e-mail marketing campaigns legally and who use e-mail as a tool to inform and communicate with their customers.

Several current legislative proposals exist to combat spam. Options include increasing the jurisdiction of the Federal Trade Commission, creating a Do Not E-Mail registry requiring opt in or opt out provisions, requiring all bulk e-mailers to have trusted identification or imposing harsher penalties on criminal spammers. Whatever the ultimate remedy, we want to make sure that the specific impact on small business is taken into account.

Over a billion small businesses use e-mail as a marketing tool, and millions use more e-mail to communicate with employees, suppliers and others critical to their business. Criminal spam cannot be allowed to prevent e-mail from its legitimate uses, and as time passes the problem will get even worse if action is not taken.

[Mr. Schrock's statement may be found in the appendix.]

Chairman SCHROCK. Right now I want to thank all the witnesses for coming today, and I would like to recognize the Ranking Member, Mr. Gonzalez. We did not know if you were going to go first or what, so you can make comments, and then we will probably have to go vote.

Mr. GONZALEZ. Thank you very much, Mr. Chairman. My apologies for being a bit late. The fact that the bells are going off now is probably good because we will get that vote out of the way. I will keep my remarks very, very brief.

Fact-finding. What is the purpose of any testimony is really for this Committee to get a better handle on what is going on out there in the small business world. Spam has created tremendous problems for individuals, government and businesses, but especially small businesses, as the chairman has already pointed out.

The question is what is the appropriate remedy? I hope that we will have many of the witnesses who will be able to tell us what they are doing and what they see for the future. The question really comes down to one of regulation and what is the proper and appropriate role for the government to play in order to achieve what would be the maximum benefit that this e-world allowed us with the Internet.

It is so important to balance I guess when you think of terms of free speech, because I do believe that some of these issues rise to the level of free speech and, as I have said, the regulatory scheme of things and then, of course, free enterprise if we can just somehow take all the factors into consideration and fashion something that makes a lot of sense.

We know the Senate has acted. We know we have bills on the House side. It is a matter of working together to really fashion something that is effective and reasonable under the circumstances so that we do not reach a critical point where we overreact. That is the greatest danger here in Congress, and that is when a crisis arises and we act quickly and not necessarily prudently.

Again, thank you, Mr. Chairman. I guess we should vote.

Chairman SCHROCK. I think we will. That is a good idea. We will go vote, do our three votes, and we will be back quickly.

Sorry, Mr. Beales. Those bells are compelling. Thank you.

[Recess.]

Chairman SCHROCK. We are told we are going to have no more votes until 1:00, but we also were told that we are going to vote all night, so a lot of silly things are going to happen today. We have one of those every once in a while, so we must endure it. Hopefully by 1:00 we will have accomplished a lot.

Before we begin receiving testimony from the witnesses, I want to remind everyone that we would like each witness to keep their oral testimony to five minutes. In front of you on the table you will see a box that will let you know when your time is up. When the light is yellow, you have one minute remaining. When five minutes have expired, the red light will appear. Once the red light is on, the Committee would like you to wrap up your testimony as soon as you are comfortable. At the six minute mark your trap door will open, so keep that in mind.

First I would like to introduce the Honorable J. Howard Beales, III, who is the Director of the Bureau of Consumer Protection for

the Federal Trade Commission. Thank you for being here, and we are looking forward to your testimony.

STATEMENT OF THE HONORABLE J. HOWARD BEALES, III, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Mr. BEALES. Thank you, Mr. Chairman. I really appreciate the opportunity to provide the FTC's testimony about spam and its effect on small businesses.

The problems caused by unsolicited commercial e-mail go well beyond the annoyance that spam causes to the public. These problems include the fraudulent and deceptive content of most spam messages, the offensive content of many others, the sheer volume of spam being sent across the Internet and the security issues raised because spam can be used to disrupt service or as a vehicle for sending viruses.

To gain a better understanding of the nature of spam, the FTC staff reviewed a sample of approximately 1,000 pieces of spam. Sixty-six percent contained facial elements of obvious deception in the From line, the Subject line or the text of the message. When these data are further analyzed to exclude sexually explicit e-mail and e-mail hawking products or services that are permeated with fraud like chain letters or cable descramblers, only 16.5 percent of the spam did not contain obvious deception and came from possibly legitimate marketers.

We further analyzed a random sample of 114 of these spam, looking behind the header information to see who had registered the domain name for any Web sites that were connected to that e-mail by a hyperlink. We found none from Fortune 500 companies, only one from a Fortune 1,000 company.

The Commission also convened a three-day spam forum. Virtually all of the panelists opined that the volume of unsolicited e-mail is increasing exponentially and that we are at a tipping point, requiring some action to avert deep erosion of public confidence that could hinder or even destroy e-mail as a tool for communication and on-line commerce.

A solution to the spam problem is critically important, but it cannot be found overnight. There is no quick or simple silver bullet. Rather, solutions must be pursued from many directions—technological, legal and consumer action.

Two key characteristics of spam make the problem particularly difficult to solve. The first is anonymity. It is possible to send an e-mail from anywhere to anyone and make it appear as if it came from somewhere completely different. Once it passes through an open relay or an open proxy that could be anywhere in the world, spam is virtually impossible to trace.

The second key characteristic is economics. For the spammer, sending out a few or a few thousand more messages is virtually cost free. Because it is so cheap, spamming can be profitable even if the response rate is very low. At our spam forum, one spammer said his business was profitable even if the response rate was as low as .0001 percent.

The panelists at the forum also discussed the damaging effect that spam has on businesses and particularly on small businesses.

Although a single piece of spam to a single consumer causes de minimis economic harm, the cumulative economic damage from spam is enormous and growing. Although there is a lack of firm research regarding cost, estimates—maybe guesses is a better word—have ranged from \$10 billion to \$87 billion a year.

The onslaught of fraudulent and offensive spam robs businesses that would like to use commercial e-mail messages as a cost effective way of marketing their goods and services. Legitimate sellers tend to be drowned out or overlooked by consumers who simply ignore commercial e-mail messages because so much spam is so distasteful.

One panelist, the president of a small ISP in Little Rock, Arkansas, stated that spam is his number one customer complaint and that addressing the increasing amount of spam is placing the very existence of his business in peril. His company does not have the financial resources and large support staff found at large ISPs. When a deluge of spam arrives, e-mail is delivered more slowly and customer complaints increase dramatically, causing the small customer support team to struggle to address complaints.

Spammers also harvest e-mail addresses from public places on the Internet such as Web sites. That poses a particular problem to small businesses because posting e-mail addresses on their Web sites facilitates the communication with existing or potential customers. In our spam harvest analyzing what on-line activities placed consumers at risk for receiving spam, we found that 86 percent of the e-mail addresses posted as web pages and in news groups received spam.

In a recent Wall Street Journal article, a market research firm reports that spam makes up 31 percent of the e-mail that small businesses receive and that fighting spam is the top e-mail priority for 84 percent of small businesses. Clearly, spam has real and significant impacts on small businesses that jeopardize the benefits of e-mail as a communication and marketing tool. These benefits can be preserved only through attacking spam through a balanced blend of technological fixes, business and consumer education, legislation and enforcement.

The Commission will continue to combat spam through its research, consumer and business education and aggressive law enforcement.

Thank you, and I look forward to your questions.

[Mr. Beales' statement may be found in the appendix.]

Chairman SCHROCK. Thank you very much.

I was sitting here listening to what you were saying. My wife handles all her parents' affairs; her parents have reached the stage where she has to handle all their business and personal affairs. She will return home tonight from California after a month, and I guarantee you she will have 1,000 plus unwanted, some of them pretty nasty things. She complains about it all the time, but does not know what to do about it.

One of the elements in the Senate spam bill includes a study of a Do Not Mail list, just like we have a Do Not Call list, and I know this is something you oppose. If you are eventually required to produce something like this, how will you protect legitimate contacts with previous or existing contacts? There certainly has been

some controversy about that with the Do Not Call and the Do Not Fax.

Mr. BEALES. Well, I think our inclination would be to approach it the same way we have approached it with Do Not Call. If you have an existing business relationship with somebody, that is a circumstance in which consumers generally expect to be contacted. They are not upset by the contact, and that would apply to e-mail as well as to the telephone so I would think that would be our starting point.

Of course, if we had to go ahead we would explore in a rule making how that has worked in Do Not Call and what changes or adjustments might be necessary or appropriate.

Chairman SCHROCK. What will enforced enhancement powers allow you to do or not to do?

Mr. BEALES. Well, our key concern about the Do Not Spam is enforceability. As I mentioned in the kinds of e-mail that we find out there, these are not people that pay a lot of attention to legal rules. As a result, we are concerned that a Do Not Spam list would not make any appreciable reduction, any observable reduction in the volume of spam that people get.

What legislation can do is we have asked for some procedural improvements that would help us get information and keep the existence of our investigations secret from the targets of those investigations.

We think we need some legislative tools that would let us better cooperate with foreign law enforcement authorities because cross border fraud is particularly a problem in spam enforcement, and we think that legislation needs to include criminal penalties for the worst of spam because too often what we find is the people we find do not have any money, so civil penalties really would not enhance our ability to go after people all that much.

Chairman SCHROCK. When you are talking about cross borders, state to state, do you see the need of federal preemption of state laws in favor of some national program that every state has to abide by?

Right now I am sure all 50 have a different process, and for people who are legitimate it is very, very confusing to them.

Mr. BEALES. Well, I think that is right. I think the Internet is by its nature borderless, and it does not make sense to erect artificial borders that people then have to figure out and worry about how to comply with. The broader the set of rules, the better.

Chairman SCHROCK. Now offshore. What could be done with businesses who send the spam offshore?

Mr. BEALES. Well, what we have done on a case by case basis is to build cooperative law enforcement relationships with foreign authorities.

In one spam case that involved the sale of domain names that did not exist we cooperated with the British authorities. One was .usa and was heavily promoted in the wake of September 11. They even sold .god domain names for a while. We shut down the operation from the servers in the United States, and they shut down the operation from there.

There is another case where we just named a defendant in the Netherlands. We have referred that case to the Dutch authorities

and are trying to help them in bringing action, so it really is a case by case attempt to build cooperative enforcement relationships, and that will become increasingly important.

Chairman SCHROCK. Of course, there is a lot of technology being developed to try to solve some of this. Do you see that technology being part of the solution to spam, or they will find something, and there will be a way for them to find to counter that? Do you see good things coming down the pike in that arena?

Mr. BEALES. Well, I think that in the long run the solutions are going to have to be in significant part technological because I think that it is very difficult to imagine any real solution if we preserve the current level of anonymity.

To change that anonymity so we can figure out who is doing it and trace e-mail back to its source, to do that is going to require technological solutions.

Chairman SCHROCK. Some of the testimony I was reading last night said there is a way that people can block being found out. You have to be able to break that logjam, and I do not know how you do that. Even the new technology I do not think can do that yet.

Mr. BEALES. I think that is correct. I think it may require changes in the basic mail protocol to make sure there is information that authenticates where it came from, but I think in the long run that is essential because whatever the solution it is going to be extremely difficult to enforce unless we can find the violators.

Chairman SCHROCK. I agree.

Mr. Gonzalez?

Mr. GONZALEZ. Thank you very much, Mr. Chairman.

Members of Congress are so fortunate because we, at least our office computers, live in a spam free world. I am going to tell you, it is wonderful.

When I go back to my campaign office and turn that thing on, it is horrible, you know, what we have to clear out because you only have so much capacity. I am not even crazy about all the stuff that the server is telling me about.

You get spoiled up here. I mean, it is just absolutely wonderful to go in there, and it is nice and clear. You are not constantly bombarded by stuff that you never asked for, are not interested in and offended by. If we feel that way, I can imagine just about anybody out there similarly situated, which is every American citizen with a computer.

It is interesting. In today's Post there is a great article, E-Mail Providers Devising Ways to Stop Spam, and they are talking about the private sector, and they are talking about the servers. It seems to me there was something you said that was disturbing, and I guess I have kind of two questions.

One of them is enforceability is going to be a problem period. I would like to think that we have established principles, legal and otherwise, that kind of point the way on how we are going to approach this, even when technology changes.

I was making a note here. At one time they used to knock on your door, right, the solicitors and such, and we tried to do something about that. Then they came through the mail. Then they

came by the phones. Then they came by the faxes. Now they come through the e-mail, right?

I am not sure what is next. You know, something in the ether world. The question really comes down to do these principles still apply in how we try to regulate unsolicited contact with citizens when it comes to the electronic age and e-mail.

The second part of my question is really the point of contact. We have to figure out where do we try to tackle this whole thing. That seems to me it is going to be the server. Of course, I am encouraged by what the servers are trying to do together to make sure, as you had pointed out, that anybody who is sending an e-mail has a legitimate address so that we can take action and then on the private sector how we establish what is a trusted sender and what is not. That can be difficult in and of itself.

What you said about enforceability. All right. We are going to be able to identify them now, which is crucial, which I will admit is crucial, but are you still going to be able to enforce it? We will be able to trace back up as to who sent it, but are we still going to have enforcement problems if we have a no spam list or if we do criminalize the act itself?

I guess those are the real questions here. Do the old principles still apply on how we try to regulate, enforce and punish? Secondly, even if we can identify it at the server point, which I think is the contact point where we can all say that is where we need to really concentrate our efforts, does it matter because whoever is in charge of regulating, whoever has a right to sue, and right now there is not a private cause of action, whether they are going to be frustrated in doing it.

Mr. BEALES. Well, I think the basic principles certainly remain the same. That is, it really is the same basic principles that apply to marketing communications in any medium. It is what we have used to go after spam so far, and we have brought nearly 60 cases against fraudulent and deceptive spam.

I do not think it is a problem of basic principles or anything fundamental, that there needs to be fundamental changes in the principles there. It is just another form of marketing. If we could find people, it could be regulated in much the same way as other forms of marketing are.

What is unique is partly the economics, but I think more fundamentally from an enforcement perspective the anonymity of e-mail. The phone system, whether it is used for a telephone call or a fax, contains information with the call about where it came from. E-mail does not work that way, and there is nothing in the message that lets us go back.

If we could go back, I do not think enforcing the law would be any harder here than it is with telemarketing or with direct mail. You know, some of those messages are deceptive. We need to bring cases and we do bring cases in those areas, but most of the companies engaged in those activities are legitimate, and we can go after and prosecute the bad actors. When we cannot find anybody, then it is much more difficult.

Mr. GONZALEZ. So until technology allows us to identify the sender, as we have the servers at the present time attempting to do

that, it does not matter what legislative scheme we come up with. It is going to be really difficult.

Mr. BEALES. It is going to be really difficult. It can be a little bit more. It can be a little bit less difficult or a little bit more difficult, but it is going to remain very difficult until we can figure out where it is actually coming from.

Mr. GONZALEZ. Thank you very much.

Chairman SCHROCK. Well, you are lucky there are only two Members here today. We thank you for being here. We thank you for your testimony.

Mr. BEALES. I appreciate the opportunity.

Chairman SCHROCK. Sure. Thank you very much.

We will get ready for the second panel.

[Pause.]

Chairman SCHROCK. Thank you all for being here. As I said earlier, the five-minute rule, if you can do that, that would certainly be a help because we want to hear what you have to say, but we also have some questions as well.

First, I would like to introduce Mr. Jerry Cerasale. He is the Senior Vice President for Government Affairs for the Direct Marketing Association. Prior to joining the DMA, he was Deputy General Counsel for the Committee on Post Office and Civil Service for the U.S. House of Representatives.

Jerry, welcome.

**STATEMENT OF JERRY CERASALE, SENIOR VICE PRESIDENT,
GOVERNMENT AFFAIRS, THE DIRECT MARKETING ASSOCIATION**

Mr. CERASALE. Thank you very much, Mr. Chairman and Mr. Gonzalez. Thank you very much for inviting me here to speak on this important topic.

The Direct Marketing Association is a trade association of 4,500 corporate members, many of whom are small businesses, and they market directly to consumers for sales or their people who help support marketers marketing.

E-commerce is very important to all marketers, especially small businesses, and there is a huge promise from e-commerce. It is a low barrier to entry. It is a way to find consumers quickly and efficiently.

There has been, however, a huge growth in Web sites, and what happened early in the Internet was that you could have a Web site up, and a search engine would find your company, and consumers could find you. The search engines now are advertising media wherein you pay to get prominence in the search find.

Many small businesses can no longer be part of that because it becomes cost prohibitive, so they have to look to go back to the old style of trying to get a list, trying to find customers rather than customers coming to find you, especially for a smaller business.

What we have is a growth potential in e-commerce of small businesses needing e-mail much more than even larger businesses. You find a list, a targeted list, and you try to reach those customers who are interested. That is the way it should work, and that is the promise of e-mail because it is so inexpensive so that entrepreneurs can get in and try to find customers that are interested in them.

There is, as my son would say, a dark side to e-mail, and the same thing that creates the promise, the low barrier to entry, creates the dark side. The dark side is it is very inexpensive. It does not pay.

If you do not care about the attitude of customers and you are looking for, as what Mr. Beales said, a response rate of $\frac{1}{1000}$ of one percent is good enough, if that is the attitude that an individual has you are not going to spend the money to target, and you are just going to flood the system with e-mail. That is the dark side. That flood comes in with pornographic stuff, sexually explicit, things you are not interested in, get rich quick schemes, Nigerian scams and, sadly, even computer viruses.

What we have to do is try and, from our perspective, save the promise. Kill the dark side without killing the promise I guess is the way to really look at it. What we have tried to show in testimony is the DMA has done a few studies to show does e-mail work? Are people at least even interested in it?

We find that 36 percent of adults in our study actually responded to an e-mail and purchased something, \$17.5 billion. Consumers alone spent \$7.6 billion, and unsolicited e-mails to prospects—even to customers—was sales of about \$1.5 billion. There were savings out of this e-mail marketing of \$1.5 billion, and even the prospects said they said in a year \$300 million, which is not tiny, especially for small businesses.

We find in our study that 21 percent of the marketing budgets for small businesses went to e-mail versus 13 percent for larger companies. Excuse me. Their Internet, not their e-mail. Their e-commerce budget. Small businesses are more dependent upon e-mail marketing than are larger businesses.

The Internet sales. Twenty-one percent of small business Internet sales came from e-mail marketing, the rest coming from Web sites and so forth, but that is significantly larger than the 12 percent that came for larger businesses.

What we need is a national standard. We have to try and avoid solutions that destroy the promise of the Internet, and destroying the promise of the Internet could be something like an opt in or even a very restrictive Do Not E-Mail list because there is no time then to try and correct the problem. People do not know the small business, the new business. They do not know them. They are not a customer of them already. You then would cut out this potential market.

We have to get rid of the fraudulent, untargeted pornographic e-mails. We hope that the House will move quickly to pass some legislation, but the big key is also not just to pass the legislation, but to provide the resources to enforce the provision.

The DMA is working with the FBI and others to try and get some money through the White Collar Crime area to try and get some enforcement, so we are doing that. Legislation is only one of those prongs, but we need it.

Thank you very much.

[Mr. Cerasale's statement may be found in the appendix.]

Chairman SCHROCK. Thank you very much.

The Subcommittee is now going to hear from Mr. Bruce Goldberg. Mr. Bruce Goldberg is the former president of Weathermen

Records, an on-line music t-shirt company based outside of Dallas, Texas.

After having several years of intensive marketing experience as an executive for Neiman Marcus, his passion for music and an eventual understanding of the Internet led Mr. Goldberg to become a very successful entrepreneur and founder and president of Weathermen Records.

He is here today to share his personal experience as to how spam has affected him as a small business owner, and, for those of you who did not see it, he was featured in a Wall Street Journal article on August 19, a fascinating article that is entitled Spam's Easy Target: Floods of Unsolicited E-Mail Handicaps Small Businesses. How Some Are Fighting Back.

I am looking forward to your testimony. Thank you for being here.

**STATEMENT OF BRUCE GOLDBERG, FORMER PRESIDENT,
WEATHERMEN RECORDS, FARMER'S BRANCH, TX**

Mr. GOLDBERG. Thank you very much. Good afternoon. My name is Bruce Goldberg from Weathermen Music in Dallas, Texas. I am here to represent my business, but, more importantly, I am here to represent all the small businesses in the United States that are powerless against unsolicited e-mail.

In college, I studied Business Marketing with the hopes that someday I would be able to work for myself and own my own company. After college, I worked my way up the ladder for Neiman Marcus, completing their executive development program and working as part of their buying staff.

I have always had a passion for music. My passion soon turned into a hobby, and I started buying and selling records at monthly music conventions. I started to keep a list of names and addresses who wanted to receive notification when I got new stuff in. Before I knew it, I was mailing out 500 of these lists a week.

I reinvested every dime I made and started to expand into music t-shirts. I put together a small mail order catalog, and before too long I was sending out 1,000 copies a month with the U.S. mail. Around the same time, I started to subscribe to a service that would allow me to communicate with people all over the world via the computer called Prodigy. Soon I was able to set up a tiny web page with a template that Prodigy supplied. This was the beginning of my on-line company.

As my customer base grew, I decided to leave Neiman Marcus to concentrate on my mail order company. When domain names were first being offered, I quickly bought up the name The Weathermen, as my company name with the marketing idea of being a music forecaster.

I invited my new customers to sign up for my free e-mail updates. My list quickly grew from the initial 1,000 to 60,000. Today, Weathermen Records is one of the largest on-line t-shirt music stores with over 50,000 regular worldwide customers and 6,000 Web sites linked to our site. We carry about 4,000 different music t-shirts from all over the world. We are still considered a small business with only three employees.

Nine-five percent of our sales and communications are done over the Internet. When I first started, it never crossed my mind that I could get an e-mail that was bulk e-mailed to me about Viagra, lowering my mortgage payment, losing weight or getting rid of my debt. Throughout the years, I started getting more and more spam, but pretty much was able to just delete it as it came in.

As my on-line presence grew, so did the amount of spam I received. I was finding that whereas most people get one of each spam, we were getting five to 10 of each, depending on how many of our e-mail addresses were hit.

The hard part was distinguishing the legitimate e-mail from junk, as I have to treat each new e-mail as a potential customer. A lot of legitimate e-mails were being accidentally deleted. Even as careful as I was, I would still lose customers by accidentally deleting their messages.

We were getting 15 spam e-mails to one legitimate e-mail. I needed to do something about this. It was getting worse. On more than one occasion, my company server was so overloaded by spam it shut itself down for several hours, costing me a day's business and its customers.

The first thing I did was to set up my account so that anything intended for ex-employees went right into the trash bin. The second thing I did was employ a spam filtering service called Spam Cop that would filter out any e-mail that was previously reported by fellow Spam Cop members as spam, and it was put into a special separate spam holding tank for spam e-mails. The problem with the service, however, is sometimes it grabs legitimate e-mail.

In an average day, the spam mail folder will keep 1,000 spam e-mails from reaching our system. Today, with all the filtering systems still in effect, we still get three spam mails for one legitimate e-mail. I spend at least an hour a day sending spam to my trash box. I get spam 24 hours a day, seven days a week.

I was recently featured in an article in the Wall Street Journal about spam. Because of the article, I got spammed. I will probably get spammed from this testimony finding its way to the Internet.

Chairman SCHROCK. Not from us you will not.

Mr. GOLDBERG. Instead of spending my time dealing with my mail situation, I could use the time to better serve my customers, increasing my profits, which in turn would generate more tax dollars for my community.

I believe something must be done about this situation that gets worse by the day. If the problem continues to grow at the rate it is currently growing, it will be impossible for businesses to rely on the Internet and e-mails as a form of communication.

I believe that people that send spam and harvest and sell e-mail addresses should be fined and prosecuted. I believe our government should try to work with other governments to abolish spam sent from other countries to try to prey on the elderly and young by means of deception.

I use my e-mail as a form of communication. Imagine if you used the telephone as a form of communication and your phone rang all day long with solicitors, but you still had to answer every call to see who it was before you could hang up because you were afraid you would lose legitimate customers.

Imagine instead of spending your time before your hearings to make sure you were prepared to serve your community you had to take that hour to weed through thousands of e-mails to find the ones that you needed to start your work day. That is what I do every day.

I also believe that if lawmakers were the targets of the same amount of excessive and unwanted spam as small businesses and had to go through all the mail themselves as a lot of small businesses do, spam would have already been outlawed.

Chairman SCHROCK. Bite your tongue.

Mr. GOLDBERG. I love my country. I grew my business from the ground up by using simple principles that consisted of good communication and providing a fair price, good quality product to people who would normally not be able to find it.

You could say that spam finally shut me down. This past week, I sold my company and am currently unemployed. For the sake of the new owner, I hope that this testimony will result in a resolution and the end of deceptive, unwanted, unsolicited commercial e-mail.

I hope whatever career I travel down next, I do not have to put up with the same frustration that plagued me and other small businessmen for years.

Thank you for listening.

[Mr. Goldberg's statement may be found in the appendix.]

Chairman SCHROCK. Thank you very much.

It is my pleasure now to introduce John Rizzi, who is the CEO of e-Dialog, a Boston based e-mail marketing firm that specializes in precision e-mail for companies like the NFL, Staples and Charles Schwab.

Mr. Rizzi has over 14 years of executive leadership in successful start up businesses all related to e-mail technology, applications or marketing services. Prior to his experience as an information systems expert, many of his leadership and management skills were gained as an officer in the Navy.

I can relate to that. I am a retired naval officer, and I think everything I learned I learned in the Navy too. Some not so good. Most of it good. Welcome.

STATEMENT OF JOHN RIZZI, CEO, E-DIALOG, INC., LEXINGTON, MA

Mr. RIZZI. Thank you, Mr. Chairman and Members of the Committee. I am very delighted to be here today and certainly grateful that the voice of the small businessman is respected in these halls.

My name is John Rizzi, and I run a business of 51 people in Lexington, Massachusetts, called e-Dialog. My business is 100 percent dependent on the effective use of e-mail as a marketing and communication channel. I am an e-mail service provider. Put simply, my company acts like the e-mail marketing department for other large companies that are really finding the relationship with their customers to be very important and certainly want to do e-mail right.

Our clients include well-respected companies like John Deere, Charles Schwab, Schering-Plough, Reuters, Harvard Business School Publishing and the NFL. In fact, if you enjoyed reading your

Redskins newsletter this morning, the one from your favorite team, perhaps the Patriots, it came from e-Dialog.

I am also a veteran of the e-mail industry, starting with a company over 14 years ago in an old laundromat that developed and sold e-mail technologies before they were available to anybody in the networks in small businesses.

For my entire post Navy career, I have been a part of the e-mail industry and in fact have been very proud to participate in the creation of the e-mail revolution. However, I am not so proud over the last couple years where our mailboxes have become polluted with spam.

E-mail is a wonderful, vibrant, economically valuable communications tool that is suffering critically right now with this infection. I could not be more pleased that so much legislative effort is going into finding a cure. What is most important now is we quickly act and stop this epidemic. The CAN-SPAM bill passed last week by the Senate is a giant step in the right direction, and I would urge the House to pass it as soon as possible.

The key value e-mail brings to businesses is that it cheaply expands their reach to customers outside their local area to everywhere in America, if not beyond. It makes them competitive with the big guys at a very low cost. For example, I personally buy tea for my wife from a company, a small shop called Special Teas in Connecticut, I buy parts for my car from 3X Performance in North Carolina, and I buy toys for my daughter from a place called Suzi's Dollhouses in Idaho.

I enjoy my relationship with each one of these customers, and I have these relationships because of the e-mail they send me. It is good for their business, and it meets my personal needs. They are all clearly e-mailing across state lines. While I do not know for sure, it is very possible that somewhere unwittingly they are breaking the law.

This binder—I had to bring a little show and tell; my daughter recommended it—contains the briefings of 37 different state laws, their anti-spam laws. On the one hand I am delighted that action has been taken. On the other hand, imagine the confusion and how overwhelmed I am and my company is to comply. This binder would scare the dickens out of Suzi and her dollhouse store in Idaho, wondering and worrying that every time she presses the Send button she might be a lawbreaker.

In my business, I have the focus and the expense of three employees that spend all day every day worrying about the state laws, industry regulations that we support and compliance and deliverability issues. I have to say, I am really glad I have these three people because when I go through this binder I get stuck at C.

I can only get that far because when I come to C, I find a state that has a hastily approved anti-spam law approved during some real political turmoil that is a disaster waiting to happen for any e-mailer in America that is trying to mail into that state and certainly any small business in that state trying to do e-mail. We have to stop that. More state laws like this are on the way. There are at least 13 more states to go.

Since e-mail is inherently an interstate medium, small businesses need one federal law that is predictable, manageable and

enforceable. The CAN-SPAM Act, with any weaknesses it may have, solves this problem. As you can tell, I am very supportive of the preemptive conditions of the law.

As happy as I am about the prospect of an anti-spam law, we have to talk about the stark reality that we face, which is the worst spammers today are already lawbreakers. If not actually breaking the law, they are unethical business people that will happily take your money for their latest form and brand of snake oil.

The trouble is that spammers can hide on the Internet. They can falsify their identities and do their work with impunity. The law can only be effective when the perpetrator of a crime can be found, and to do that we need technology.

I am happy to say my company is part of an industry group of legitimate e-mail marketers called the E-Mail Service Provider Coalition, nearly all of these businesses small businesses, that are working together to develop a universal technology to provide an authentication system for large e-mailers that will effectively remove the hidden identities of spammers.

I brought copies of a white paper about this issue called Project Lumos which I would offer for review and to be entered into this record. Simply, either the sender of the mail will be automatically authenticated as an identifiable and legitimate e-mailer or the mail does not go through. This, combined with other initiatives, will drive spammers out of their holes where the law can find them.

Coincidentally, as Mr. Gonzalez mentioned, a very good article about this is in today's Washington Post.

I and my colleagues in the industry are extremely confident that this will work, and it is only months ago. We need to be realistic that this is part of the solution, and the law alone cannot solve the problem.

The final critical factor for the protection of small businesses is the subject of a Do Not E-Mail registry. I have to admit, this sounds intuitively obvious and like a good idea, but I have to tell you with all my experience that this is a disaster waiting to happen, especially for small businesses.

Look deeply, and you will find enormous technology challenges that small businesses will not be able to adopt. You will see security challenges that if compromised will allow this big list to go into the wrong hands, and I dare say you will be spammed within hours, if not minutes, when that happens.

You will see business people confused as to why they can mail fewer and fewer of their customers, and you will see consumers frustrated and confused when they are getting less and less mail from their favorite companies, but no less spam. Remember, spammers are lawbreakers. They are not going to take their lists and match it and clean it against a registry. They are already breaking the law.

The good guys will do it though, so they are going to have fewer and fewer people to mail to, but no one will get any less spam. The Do Not E-Mail registry I am afraid will backfire, and small businesses will lose.

To summarize, please act quickly and approve the CAN-SPAM bill that came from the Senate. Give the industry time to develop the technology that will make spammers identifiable, support con-

sumer education on how to avoid spam, and, very importantly, please do not hurt small businesses by mandating a Do Not E-Mail registry.

Thank you.

[Mr. Rizzi's statement may be found in the appendix.]

Chairman SCHROCK. Thank you. I like the idea of your Redskins thing, but my guess is Mr. Gonzalez would prefer the Dallas Cowboys, right?

Mr. RIZZI. We do their newsletter too.

Chairman SCHROCK. It is my pleasure to introduce Catherine Giordano. Catherine is the president and CEO of Knowledge Information Systems, which is a Virginia Beach based technology training and research firm. She is here today representing Women Impacting Public Policy, WIPP.

Ms. Giordano has more than 24 years' experience in the operation, management and coordination of major projects, management, supervision and training of personnel.

I have known Catherine for many years. We live in the same city. When I first decided to run for the state Senate, she was one of the first people I went to. She gave me that are you crazy look then, and when I saw her at breakfast this morning that look was still on her face.

We are glad to have you here, Catherine. Thanks.

**STATEMENT OF CATHERINE GIORDANO, PRESIDENT AND CEO,
KNOWLEDGE INFORMATION SYSTEMS, VIRGINIA BEACH, VA,
ON BEHALF OF WOMEN IMPACTING PUBLIC POLICY (WIPP)**

Ms. GIORDANO. Thank you very much. Good morning, Mr. Chairman and Mr. Gonzalez. My name is Catherine Giordano. I am the president of Knowledge Information Solutions, Inc. located in Virginia Beach, Virginia, and I am appearing today on behalf of Women Impacting Public Policy, a national bipartisan public policy organization advocating on behalf of women in business representing 460,000 members nationwide. I serve as co-chair of WIPP's procurement committee.

K.I.S., my company, is a woman-owned, 8(a) certified small business which employs 47 workers. We provide computer products and IT services such as ISP Internet and wireless connectivity and network design and consulting. We supply IT products and services to the federal government through 11 government wide acquisition vehicles to approximately 47,000 customers.

I would like to thank you, Mr. Chairman, for inviting me to speak on a subject that my company deals with on a daily basis and one that I believe is very costly to small businesses—spam. Coincidentally, KIS just recently completed an internal analysis of the effect of spam on our business, so this testimony is timely to our company.

Most business environments are now computer based and dependent on e-mail as the essential form of business communications. At KIS, our small business is reliant on a communication system to our customers that is by electronic mail and correspondence predominantly through computer technology.

Small businesses are always interested in attracting new customers, and we are ever mindful and concerned about annoying

current or prospective customers. Therefore, KIS offers a form of permission based customer marketing that will readily remove their name from any KIS mailing list upon request. This practice is typical of most other small businesses. Legitimate businesses take these requests seriously and honor requests to remove names from the list.

Unsolicited commercial electronic mail, spam, represents 30 percent of KIS' inbound correspondence. It is an ongoing process, and it becomes more expensive as the innovation of global spam capabilities has shifted the burden of cost from the sender of the spam to the small businesses, ISP providers and the customer.

Since spammers continuously change their methods of operation, we spend additional employee time to find just the right mix of settings to adjust. Our review shows that KIS' small business customers spend an average of seven minutes per day per person dealing with spam.

Since KIS provides 250 small businesses in the southeastern Virginia region information technology management and ISP support services, we estimate that the total cost in lost productivity to these customers is estimated to be \$2.9 million annually. Mr. Chairman, \$2.9 million could be used much more productively by small businesses on items such as equipment purchases, creation of jobs or providing health care to employees.

The spam filtering methods KIS currently utilizes is DNS or domain naming services, the protocol for translating names into IP addresses. For example, an address like www.google.com must be converted into a numeric 216.239.41.99. One of the options to filter spam through DNS, called blacklisting, typically catches only 25 percent of these e-mails. Filters utilizing key word searches will catch an additional 5 percent of the e-mail.

The number of false positives, which are e-mails that are wrongfully identified as spam, raises daily as more and more companies are inadvertently submitted to blacklist servers. Of these e-mails caught by DNS blacklisting, the keyword searching, two to five percent are false positives.

The cost associated with identifying false positives is roughly \$2,499 annually and an estimated yearly cost of employee productivity after KIS current anti-spam measures to my company is an estimated \$93,750.

To implement a KIS internal, full-blown, perimeter e-mail server incorporated spam detection system costs our customers \$4,500 plus the cost of equipment. Their return on investment after implementation of a full-blown spam detection software is estimated at 5.5 months, and that only catches 85 percent.

As the Committee knows, the Senate in the last several weeks passed an anti-spam measure by 97-0. Although WIPP has not had a chance to review the proposals pending before the House in depth, our thoughts are twofold. One, spam is a costly expense for small businesses. Two, when enacting legislation to limit spam, Congress should take into account the effect of its actions on small businesses for compliance.

When considering a new law to prevent spam, our members do not want the burden of seeking permission from every customer in order to send an e-mail. The FCC's proposed legislation on the Do

Not Fax rule is a good example of good intentions by the government agency, but had consequences for small business. The proposed rule would require every business to seek permission from every customer before faxing things like invoices and other necessary business communications.

We have heard from our small businesses, and they are simply not practical when trying to restrict unsolicited faxes. Similarly, such a system for e-mail communications would be onerous for small businesses. Compliance with an opt in is problematic for small businesses with limited resources.

In closing, I would like to paraphrase a quote from Ms. Paula Seles, Senior Counsel, Washington State Attorney General, delivered before the Committee on Energy and Commerce on July 9:

Strong legislation is only one part of the solution. If legislation is passed, it must be flexible enough to allow new technologies that may ultimately be more effective than any law. There is no easy fix to this problem, and it will take all the tools we have to address it.

Ms. Seles' statement summarizes WIPP's approach on spam. There is no question in our minds that limiting spam is good for small businesses. The solution, however, must take into consideration the compliance cost to small business.

Thank you.

[Ms. Giordano's statement may be found in the appendix.]

Chairman SCHROCK. Thank you, Catherine.

We are voting. Mr. Ham, Mr. Crews, the two votes will be quick. We will be back and then let you do your testimony.

I am sorry. I thought for sure this would not happen until 1:00, but anything happens. We will be right back.

[Recess.]

Chairman SCHROCK. My apologies, and thank you for your patience.

Mr. Rizzi, we would have never allowed this in the Navy, would we?

Mr. RIZZI. No, sir.

Chairman SCHROCK. It is not efficient.

We are going to hear next from Shane Ham. He is the senior policy analyst for the Technology and New Economy Project at the Progressive Policy Institute here in D.C. He Progressive Policy Institute is a think tank affiliated with the Democratic Leadership Council. Mr. Ham writes and lectures on a number of technology and new economy policy issues.

We are glad to have you here, and thanks for your patience.

**STATEMENT OF SHANE HAM, SENIOR POLICY ANALYST,
PROGRESSIVE POLICY INSTITUTE**

Mr. HAM. Thank you, Mr. Chairman. At the Progressive Policy Institute, we have been advocating for the advancement of the Internet economy for six years because we think it is important to the future growth of the entire U.S. economy, and that is why for almost that long we have been pushing for spam control. We have been involved in this debate since all the way back in the 1990s, back even when the DMA was opposed to legislation on it.

We have been moderate on the subject. We have never called for a complete ban on all unsolicited commercial e-mail or for an opt in standard, which is effectively the same thing as a complete ban because if you have opted in it is no longer unsolicited e-mail. I feel that if you opt in it is no longer unsolicited. You say I am requesting the e-mail, so it cannot technically be spam anymore, which that is the same thing as a ban.

I think the opposition to an effective spam legislation by the marketing industry and others is increasingly becoming a Pyrrhic victory. We now have a patchwork quilt of state laws that it is very, very difficult for businesses to comply with. There is a law out there in that seaward state that is going to just give all e-mail businesses fits.

I think, more importantly, the real tipping point that we are looking at now in spam is that people are beginning to understand and become upset about the fact that spam is destroying the entire e-mail system in general.

A recent report by the Pew Internet Foundation, and I cite this in my written testimony, indicates that we are now officially at the point where more than half of Internet users believe that spam has caused them to trust the e-mail system in general less, and I think that is a real tragedy.

It is becoming harder and harder for moderates like us to find a balanced solution to the problem that will, you know, benefit consumers, that will benefit Internet users and protect the people who rely on e-mail to run their businesses and their small businesses.

I think when you are thinking about what to do about spam with regard to small businesses, there are a couple things you need to keep in mind. First of all, it is perfectly clear, as we have heard already today, that small businesses are much more the victims of spam than they are ever going to be utilizers of spam in order to grow their businesses. It does really more harm to small business overall than it could ever really do good.

The main reason for that obviously is that small businesses cannot take the steps to protect themselves that individual users can. You cannot have a white list that only lets your friends and family e-mail you because you have to get e-mail from complete strangers if you want to grow your customer base. You cannot just set up a filter that throws out anything that is vaguely suspicious because you will be throwing out customers too.

That is why I think, as Howard Beales said, 84 percent of small businesses say that fighting spam is their top priority, but not nearly that many would say continuing to spam themselves as a business strategy is a top priority.

I think another problem that small businesses face is that it is getting harder and harder for the average Internet user to distinguish between legitimate and illegitimate spam. That is increasingly becoming a false dichotomy.

There is a clear legal line between fraudulent and non-fraudulent spam, and there may be a moral line between senders who follow industry best practices and those who do not, but to the average users they are just distrustful of any kind of unsolicited e-mail that they find in their in box in general.

The idea, as Jerry was citing some numbers about how many businesses are using e-mail in order to expand their customer base, but I think you will find as the spam problem continues to get worse and worse and people trust the system less and less, there will be fewer and fewer people that are willing to respond to spam not only to make a purchase, but even to do something like click an opt out link as it becomes more and more clear that clicking that link that says Remove Me From Your Mailing List is a good way to get 10 times as many spam as you were getting before.

People are just going to completely tune out from it, and it will, I believe, disadvantage small businesses because the only kind of e-mail marketing that is going to work is going to be from the large, brand name firms that people already know and trust, but trying to find new customers for a small business that nobody has ever heard of, tragically those small businesses are going to be lumped in with the scam artists and the pornographers and all the other spammers that end up straight in the trash.

We have over the years advocated different solutions, but we think that we have gotten to the point where we really need to take a radical look at this. The problem has just gotten too bad to take the smaller steps that might have worked four or five years ago.

The Do Not E-Mail list is one that has been talked about a lot. I know that even the FTC is opposed to that, and there is no doubt that there is tremendous technical problems with implementing a Do Not E-Mail list, but we still think it is a good idea, but it has to be done completely.

The way it happened in the Senate bill that just asked the FTC to do a study and then sort of gave them permission to go forward with it if they so choose after the study is not going to work. It is going to take significant research with probably millions of dollars to hire the staff and equipment that will be necessary to keep a Do Not E-Mail list safe from hackers and from spammers.

The other thing that PPI has long advocated, and we really think this will work, is requiring a standard label in the subject line identifying spam not just for pornographic e-mail sent to make it automatically filterable, but for all e-mail that fits the definition of unsolicited commercial e-mail.

All three of the major bills right now just indicate that there has to be a clear and conspicuous—it has to be obvious basically that an e-mail is spam. You cannot make the subject line fraudulent. That is not going to allow technology in the computerized, automated filters to do the work that is necessary to keep the spam out of in boxes and protect small businesses from the flood of spam in their in boxes that they have to wade through.

I think that everything else, you know, regarding private right of action, those are details that can be negotiated. I think preemption is something that everybody is in favor of, but if we do not get I think these two things, a truly effective Do Not E-Mail list and a standard label for all unsolicited commercial e-mail, I do not think we are actually going to solve the problem.

Thanks for your time.

[Mr. Ham's statement may be found in the appendix.]

Chairman SCHROCK. Thank you very much.

Wayne, you are a very patient man. Wayne Crews is the Director of Technology Studies for the Cato Institute. He is an expert on new economy regulatory issues, including antitrust policy, privacy, spam and intellectual property.

Before he went to Cato, he was the Director of Competition and Regulation Policy at the Competitive Enterprise Institute, and we are glad to have you here. Thank you.

STATEMENT OF WAYNE CREWS, DIRECTOR OF TECHNOLOGY STUDIES, CATO INSTITUTE

Mr. CREWS. Thank you. It is my pleasure. Good morning, Mr. Chairman. I appreciate the opportunity to appear today.

Chairman SCHROCK. It used to be morning, but it is not anymore.

Mr. CREWS. It is afternoon now. We can have some Spam for lunch.

The increasingly apparent downside of an Internet on which you can contact anyone you want is that anyone can contact you. The openness that was once central to the Internet experience, as the marketers like to call it, is now a drawback.

However, the dilemma is not just that legislation likely will not rid us of spam, given the net global pool of scofflaws. Rather, legislation like ADV mandates and Do Not Call lists still do not address the root problem of spam. One, the lack of authentication of senders, and, two, the ability of spammers to shift the cost of bulk e-mail to the recipients.

Clearly, such misdeeds as peddling shoddy goods, forging the name of the sender and phony unsubscribe promises should be punished. Abuses like dictionary attacks and spoofing often commandeer unwitting computers, and they resemble hacking more than they do commerce.

To a great extent, these are already illegal, and alternative market driven solutions by a technology pricing and industry consortia are going to become more urgent. Maybe that is a blessing in disguise because spam is not a single dilemma. Kids seeing porn in the in box is a different problem than ISPs overwhelmed with ricocheting Viagra ads.

Moreover, the industry must coalesce to address cyber security and hacking concerns that need remedying perhaps more urgently even than spam. Actually solving such problems is a different proposition from passing a law.

Proposed legislation, for example, would impose subject line labeling like ADV for commercial e-mail, mandate unsubscribe mechanisms, ban harvesting software, set up fines or even bounties and contemplates an extensive and likely hackable, in my view, Do Not Spam list.

If the legislation merely sends the worst spammers offshore, we have only created regulatory hassles for small businesses trying to make a go of legitimate commerce and mainstream companies that already followed best practices like honoring unsubscribe requests.

Proposed legislative penalties can easily keep many small businesses out of Internet marketing altogether for fear of a costly misstep. Is that our goal? Commercial e-mail, even if unsolicited, may not always be unwelcome, yet how might the definition of

spam expand after legislation? Is it just bulk unsolicited commercial mail, or is it anything you did not ask for?

Numerous questions arise. Many e-mails are not commercial, but are still unwanted—press releases, resume blasts, political and charitable solicitations. I have even seen the term scholarly spam used for e-mails sent by groups like my own. Even the signature lines we all put in our e-mails are a subtle solicitation, whether we admit it or not. If we need ADV for advertisements, why not REL for religious appeals?

We should not discount the creativity of lawyers looking to sue the easy marks in the wake of legislation like the small business that will inevitably slip up when he is implementing an unsubscribe request or trying to adhere to the Do Not Call list and Do Not Spam list and makes an error.

Navigating e-commerce regulations after legislation like this could be relatively easier for large firms, and that is something to consider with regard to small business impact. Much of the marketing industry's newfound support of spam legislation seems defensive and aimed at protecting the ability to send legitimate commercial e-mail. That is understandable.

Post legislation, marketers are surely going to feel that they have met federal requirements like ADV and a street address. Therefore, ISPs have no right to block their messages. One cynic said that the CAN-SPAM Act meant that you can spam.

Blacklists, despite their problems, are one of the key means of dealing with spam today. Contracts and rights of ISPs and consumers to end unwanted relationships, rather than federal guidelines, still need to play a big role in the future, especially as technology catches up with the problem.

There is some good news. If your fundamental desire is to stop spam totally in your personal in box, you can do it already using a handshake or a challenge and response account, and that might be something we talk about later. There is a movement in the industry towards that.

Meanwhile, the entire industry needs to get busy on standards such as digital signatures or seals for trusted e-mail as a means of helping tomorrow's ISPs block spam, but it could require unprecedented industry coordination. At bottom, the flat fees and free e-mail of today are not a fact of nature or natural right.

Ultimately, e-mail postage or protocols that allow ISPs and users to charge fractions of a cent for unsolicited mail would allow users to impose their own conceptions of spam. Emerging bonded sender programs anticipate this kind of sea change.

It may be that today's e-mail system in which originators of messages remain anonymous is altogether inappropriate for the commercial information society of tomorrow. While the government must not outlaw anonymous e-mailing, maybe it needs to be impossible, not merely illegal, to send a commercial e-mail if the network owner cannot discern who you are or charge you. If so, those are jobs for the industry that cannot be replicated by passing a law.

Thank you very much.

[Mr. Crews' statement may be found in the appendix.]

Chairman SCHROCK. Thank you, Wayne, and thank you all very much.

If we do not get this spam under control, what do you see as the largest long-term effect on your businesses? Obviously Bruce Goldberg, we heard what happened to him. Are we going to hear more stories like him or what? I am curious what you might think.

Mr. CERASALE. If I may start, Mr. Chairman, I think you are going to get a growing lack of trust and lack of use of e-mail. What is happening today is there is so much spam. Even from large companies, a legitimate e-mail that is a confirmation of an order is not opened because they are just being deleted.

I think from the point of view of looking at it at the consumer's side, you are going to see the non-economic, non-commercial use of e-mail from the consumer side, and I think that that is a real problem that faces all marketers trying to use e-mail.

Chairman SCHROCK. Bruce?

Mr. GOLDBERG. I believe the problem, in my opinion, keeps growing because there are a lot of companies out there who see how easy it is to get away with it, and they just keep jumping on the bandwagon whereas before they would not do it. Now they see how easy it was.

I had one company that sent me an e-mail about selling beepers, beeper service, free beepers. They put their 800 number in there. I decided to call them to see what they would say.

I called them, and I said do you really sell beepers through your spam e-mails? I mean, are people that stupid that they would trust you by going through this? They said yes. I mean, we get tons of orders every day. I was amazed. I was thinking wow, maybe I should do this.

Chairman SCHROCK. We will have you up here for a different reason, right?

Mr. GOLDBERG. I mean, there is still the ethical belief that I do not think it should be done, but I just think that a lot of people are jumping on the bandwagon because they see they can get away with it, and it just keeps multiplying every day more and more. It is never going to end.

Chairman SCHROCK. John?

Mr. RIZZI. The line between being a good e-mailer and a spammer are getting blurrier and blurrier every day. We see companies frozen with making their decisions about how to do e-mail right, even companies with budgets to do it, because they do not want to be mixed up in the mailbox with all the Viagra ads and so on.

Already there is an impact on business. There is an impact on our business with clients that are slowing down or just freezing where they are as far as how much mail they want to do.

Many companies today that, you know, were heading down that path to doing e-mail more effectively have stopped to wait to see, you know, what kind of technology comes out, what kind of legislation comes out. The future is very predictable. There will be less and less and less of the good stuff.

Chairman SCHROCK. Catherine?

Ms. GIORDANO. From my perspective, it would be the fact that we communicate with our customer base through the system itself, and it is usually marketing information that they have requested.

We have become more and more hesitant to do that kind of communication, but I can tell you it is very onerous on a business owner to have to stop that ease of communication and pick up the phone, call the individual and say I am now going to fax you this information. Will you pick it up on the other end so it is not considered a junk fax? It is usually information they have requested.

The second thing it is going to do for me is I now currently have one person dedicated—it is actually one and a half people dedicated, about a \$40,000 a year salary—to monitor this system, and I am going to have to add additional people to just take the load to monitor what we receive and what we receive for our customers.

It is kind of a double edged sword for me. It means I cannot do business as usual, and it means I have to spend more money to assist the small businesses that are receiving the other end of that burden.

Chairman SCHROCK. Shane?

Mr. HAM. I think over the very long term probably the worst case scenario would be sort of a Balkanization of the entire e-mail system. Rather than having the simple open system that we have today, more and more people will start to get into little mini e-mail systems that only their friends and family are in and leave everybody else out. The e-mail as we know it just will cease to exist.

Chairman SCHROCK. Wayne?

Mr. CREWS. You can see I am skeptical of legislation, but it may come to pass that we need—the states, 30 of the states, already have legislation, and the e-mails are still coming in. It is not stopping it. We may see that ramp up to another level if things go global and the e-mail still comes in.

You are already seeing some of the big players take new steps that they could have taken a long time ago, in my opinion, and I think if the industry does not get its act together and solve this the legislation is going to come and be more onerous with limiting the amount of outbound e-mail that an individual can send, things of that sort that you have seen, or if you do send e-mail and your pattern changes you suddenly get a challenge response, a challenge from the provider, things of that sort.

You are seeing those kinds of things start to happen. You are seeing movement on making a seal work or a trusted sender seal work. It is a tremendous undertaking. I have heard that kind of thing be compared to widening all the nation's roads six inches.

On the other hand, if that is what Commerce requires, if it is the case that an anonymous e-mail system like we have is unsuitable for a commercial world where you have to do a lot of things, you want to do your anonymous speaking, but you have to have secure commerce. You have to have financial transactions, insurance, purchases, all kinds of things.

It may be that we are still six years into the popular Internet, and if we need to make those fundamental changes they need to be thought about now. We should be careful that legislation does not unintentionally make folks say well, the government is taking care of this problem. We do not really worry about moving forward.

Chairman SCHROCK. Unfortunately, the government would probably just add to the complication of the thing if they did it.

You peaked my interest when you said handshake. Would you go into that briefly?

Mr. CREWS. Okay. It is not an answer for everybody, but I will just mention it really quickly. I am sure a lot of the folks on the panel already know what it is and folks here know what it is, but for two and a half years I have had an account like this.

EarthLink has just come out with a major roll-out of what they call a challenge and response e-mail system for its users. In other words, you sign up for this account. You can dump your white list in, all of your contacts and things of that sort. Any of those who e-mail you will come through.

If you get any e-mail from a stranger, that stranger gets a response not from you, but from the system, that asks him to enter a certain password that is generated there or look at an image because typically a spam box cannot decipher images and things like that, and then put that into the reply, and then the message will go through. That stops spam.

In two years, I have not gotten a spam in that account. It does not mean I will not. It does not mean you cannot set up, you know, spam sweatshops where people just answer the challenge. It can still happen, but in general what it does is it changes the focus. In a way it is a proof of concept. The reason we have spam is because it is costless for the sender.

In a way a challenge and response, despite all of its problems, because it throws wrenches in the mailing list and things like that, because it causes real problems there, but it is a proof of concept that if you shift the cost back to the sender it does put a real damper on what they do.

Now, if I am an individual and I have this at home, I do not want my kids to see, you know, an unprotected e-mail account pop up because now they contain graphics and everything. This protects you from that.

If you are a business and you need to get solicitations from customers, you need to get customers to come right through or if you are a media company and you need press releases to come right through, it is not going to be appropriate for you.

Then again, as time goes by, maybe it will be. The ethic may very well change from everything comes in unless you say no to nothing comes in unless you say yes. That is what challenge and response does.

Remember, once you do it you only do the challenge one time. If I get an e-mail from a stranger and he answers the challenge, any future e-mail he sends me will come through without being impeded so long as I have not blocked him, so every for businesses it might be appropriate if they think their customers are willing to put up with that.

Chairman SCHROCK. So you have the choice of whether to block or not to block?

Mr. CREWS. Right.

Chairman SCHROCK. All right. You are all familiar with that, I guess.

Mr. Gonzalez?

Mr. GONZALEZ. Thank you very much.

The first thing I want to point out is that we really appreciate your testimony and your patience. Many times we have the witnesses, and they only see a couple of Members up here and get discouraged. Please understand that your testimony forms the basis for a lot of things that we do here because obviously we are taking it down. It is being recorded. Your written statements will be disseminated among all of the Members.

When I was voting, I saw Ranking Member Velazquez, and she reminded me that we were having an Hispanic caucus meeting and I was on the agenda. Of course, she understood that I was here. This is our first priority.

Please understand that the Chairman and Mr. Manzullo and the Ranking Member, Congresswoman Velazquez, will join us in thanking you for your presence here this morning. It is very, very important, and it is a great education.

I am going to start off with maybe benchmark things that we can agree on, things that are not clear even in my mind. The problem that Congress faces right now is that we do have a cure, as they say. The good news is that we have a cure. The bad news is it kills you. That is the real fear.

I think Mr. Crews understands what I am talking about. It is a delicate balance, as I have already said, and I am hoping that we move quickly because if the market does not do it then the abuses, and we reach the crisis, and then we overreact.

The first thing I am going to ask all the witnesses is what is your definition of spam? I am getting the impression that they will be different. Maybe I am just wrong about that.

I will start with the first witness. Is it Mr. Cerasale?

Mr. CERASALE. Cerasale. Mr. Gonzalez, thank you. We have tried to define spam, and you get even within our membership lots of different versions. I think that the way we look at it, it is unsolicited, bulk, untargeted e-mail.

Some people would add there is fraudulent stuff in it, but that is probably just a fact that it is that. Ninety percent of the spam that comes into AOL I have heard them testify violates some current law already, so I would say you would look at bulk, unsolicited, untargeted e-mail.

Mr. GONZALEZ. Thank you.

Mr. GOLDBERG. I have to agree. The mail does not necessarily have to have a deceptive product in it because I have seen some legitimate e-mails come through, but it is just anything that basically comes out that you do not ask for that can go to like if it hits a domain they can put 100 different @theweathermen.com, like they can put sales, owner, webmaster, Mike, John, Steve, and you will get every single one of those. That is I guess what I would consider it.

Mr. RIZZI. It is definitely a challenge to define spam. Often it comes down to a question of opt in versus opt out. In our industry, many, many think tanks and many, many resources have been spent on the question of opt in versus opt out. I have to tell you, it is very important and largely academic until we can find the spammers.

There are 100 definitions that are important. The fact of the matter is lawbreakers do not care, so we have to find a way to

identify them, and then once we identify them we can start dividing it down to well, was this spam or was it not, and was it opt in or was it not.

There are technologies that can be developed that can even have triggers in them for that level of sensitivity, so I think that is where we need to head, but it is still very hard to define.

Ms. GIORDANO. In my business microcosm, the best way to define it is if it does not relate to my business environment, it is spam. That is how I have defined it for the folks that actually monitor our system.

We have received everything from solicitations from people in foreign countries to help them because their father died and they need money and will you please enter your bank account number, like I am really going to do that, to the Viagra ads or sunscreen. You name it, it comes in.

They know that from a personal perspective in my little space, which is KIS, whatever does not relate to my business does not belong there. Therefore, they block.

Mr. HAM. I think that a key element of spam is it definitely has to have a commercial purpose, and it has to be unsolicited in a sense not only that it was not asked for, but from a business that you really had no prior interactions with.

If you have been given a chance to opt out in a previous interaction—if you were to go to TicketMaster and buy concert tickets and you are given a chance to opt out and you choose not to do so and then TicketMaster sends you an e-mail saying guess what, your favorite band is coming back to town, even if I never really wanted that e-mail in my in box it would not be spam because I had the chance to avoid it and chose not to do so.

Mr. CREWS. I agree with a lot of what I have heard here. I mean, the definition of spam can vary, and it can change over time. I mean, as commercial solicitations, if they were to go down, you can imagine non-commercial ones would increase.

The key point, though, is it does not matter how legislation defines spam. People need to be able to define it themselves and decide what they are going to filter out. I mean, even ISPs filtering out and blacklisting things, you know, is one of the big hammers we have now to deal with the problem, but you can lose important messages that way.

The more individuals can decide through trusted sender or through eventually if there is a way to charge to look at an unsolicited mail, ultimately the road you want to go to is to let people decide for themselves, and you want to make sure the legislation does not in any kind of way impede that.

I will just point out something extra on the Do Not Call list because it occurred to me as I was hearing some of the commentary on it that there is a big reason why it would not help. If one of the main problems we are having now is dictionary attacks, it would not matter that you put your name on the Do Not Call list because the bad guys are simply going to go johnsmith1, johnsmith2, johnsmith3@yahoo.com, and it is not going to matter if your name is on the Do Not Call list.

Ultimately people have got to be able to filter out all of that kind of stuff that is going to come through, and it is going to require industry getting its act together.

Mr. GONZALEZ. I guess the important point is that I am not sure that Members of Congress—we all have our own definitions of spam, just as you do. I think it is important what Mr. Crews pointed out, and that is you give the consumer, the citizen, the ability to define spam in their own world and then to proceed to exclude that which they equate to spam.

I mean, that is the perfect world if we can reach it, and we have to remember that because that which empowered really Mr. Goldberg to be a success very well would be complained by others because they are being solicited for one reason or another about music t-shirts or whatever the business was. We do not want to do that. We want to see more success stories like Mr. Goldberg.

Let us see if we can agree on something that is basic. Do we all agree, and then go down, and you tell me if any of you disagree, that there has to be a federal preemption so that you do not have to deal with 50 different sets of rules? I mean, we do that all the time, and you already know what it is like.

Do we all agree that we are going to have to have some sort of sender ID mechanism, and the technology has to be there for the enforceability portion of it—also, it allows some filtering and such—and that we should not have an opt in because that would be unworkable?

I will just start again. Mr. Cerasale?

Mr. CERASALE. I agree with those three points.

Mr. GONZALEZ. Okay. Mr. Goldberg?

Mr. GOLDBERG. Definitely. I agree, too.

Mr. GONZALEZ. Mr. Rizzi?

Mr. RIZZI. I agree.

Mr. GONZALEZ. Ms. Giordano?

Ms. GIORDANO. I agree as well.

Mr. GONZALEZ. Mr. Ham?

Mr. HAM. I agree with all three.

Mr. GONZALEZ. Mr. Crews?

Mr. CREWS. I am just putting on my legislation critic hat, that is all.

You know, federal preemption is something debating in a lot of areas in on-line privacy and all sorts of areas, but again just passing the law or setting up a Do Not Spam list or mandating the ADV, it does not do any good to preempt the states with that kind of law if it is not doing any good. That is my only concern.

Mr. GONZALEZ. But if it is a good law, in other words, the best that we can fashion—

Mr. CREWS. As I said in the testimony, you go after the bad actors, the fraudulent stuff. If someone is impersonating someone else in an e-mail and things like that or impersonating another domain name, things of that sort, sure, that is appropriate to go after, but it is not something that can be micromanaged in any kind of way.

You have to be careful about ADV requirements and Do Not Spam list requirement and their impacts on small business and

who can manage that, you know, whether that is something that a small company can really deal with.

Mr. GONZALEZ. Okay. Thank you all very much.

Chairman SCHROCK. Let me follow on to what Mr. Gonzalez said as it involves Congress. What is the worst thing that Congress and the FTC can do in this situation? So many times we create legislation here that we think is going to help, but we think there are so many unintended consequences that we do more harm than help.

That is why I, frankly, wish the market would take care of this instead of people in Washington because you know when Washington gets involved it is probably going to put more hamstrings on you than you want.

What is the worst thing that we could do so we do not do it?

Mr. CERASALE. Okay. Because of what has happened in your home state, I think if you do nothing would be very problematic because California's law, which will go into effect on January 1, will effectively put an opt in regime across the nation because of the way the law is set up that you violate it even if you send an e-mail to an account that is billed in California.

For example, I live in California. My son is in college in Connecticut and uses my AOL account, which is billed in California. If you send an e-mail there, that would be a violation. There is a real problem.

Chairman SCHROCK. You have to rethink that, letting your son have your AOL account.

Mr. CERASALE. That is true, but that is a problem. I think doing nothing would be awful at this point in time, not preempting California.

The Do Not E-Mail list also just is not going to work. There is no way to keep it fully secure because if I give you a list with two million e-mails on it and someone scrubs it for me and I get back a million e-mails that are not on the list, I sudden have at least a million e-mails that are on the list because I have the old list, so it does not even need to be hacked to be able to get that list.

Chairman SCHROCK. Bruce?

Mr. GOLDBERG. I believe that the solution would be that I do not think that unsolicited e-mails should be completely banned because a lot of problems will come into play.

I had my server hacked into one time. I have an open script in there. I am not an HTML expert, but somebody somehow got in and found a loophole in my system where they can send their e-mail out using my system to make it look like it was coming from me.

When I reported it to the ISP that I use, they basically said well, you need to tighten up that hole that is in there so that they cannot send out mail anymore. If there was a Do Not Spam list—I mean if there was an unsolicited law, I would have been probably in a lot of trouble for that, even though I did not even know it was going out.

I think that the solution, in my opinion, is somebody needs to come up with some kind of technology kind of like what EarthLink is using to just kind of—you know, a nationwide, across the board everybody uses the same thing.

I know a couple states now have a thing where if you call you have to identify yourself. If it does not recognize your name, you have to say who you are, and then the person on the line gets to decide whether or not they want to take that call.

I think that if all the states did that with e-mail, I think that we probably would not even have to go any further with the Do Not Call list or anything like that because somebody came up with a product that already took care of the situation before it got that far.

Mr. RIZZI. I would agree that doing nothing is the biggest problem, particularly because of preemption in all the states, the 37 states now. The California situation is very threatening to the business.

Let me give you a little anecdote about Utah. Utah has a private cause of action condition in their law, which means pretty much any lawyer can go after anybody that may have made a mistake in the way they sent their e-mail. If there is even one percent of the small businesses in America that understand that that law exists when they are mailing somebody in Utah, I would be surprised. It does not happen.

What has happened there is that one law firm in Utah has now placed over 1,200 lawsuits. One law firm. Most of the people that have received this spam are staff members of that law firm, and they were simply what we refer to in the industry now as "spambulance chasers" and going after—you know, it is no different. Going after small businesses that do not have the resources to do the investigation, hire their lawyers. It is much easier to comply and submit and write their check and say go away.

That will happen more and more. I am sure there are just stacks of lawyers in California right now wringing their hands for January 1 to put on their own "spambulance" process, and that is a problem. There will be millions of small businesses breaking the law on January 1, and they will not know it.

Chairman SCHROCK. Unintentionally.

Mr. RIZZI. Completely unintentionally with their heart in it like Bruce here to go do the right thing for their customers, but they will not know it. They will be breaking the law.

Legislation, if it does not happen in this session, our industry and small businesses everywhere are going to be lawbreakers.

Chairman SCHROCK. Catherine?

Ms. GIORDANO. Big ditto on that. My 47,000 customer list is not contained within the borders of Virginia, and my biggest fear is that what it will do if there is not some uniform code of compliance. I am not sure I understand what the uniform code is.

I would like it to be a technological advancement that would rid the problem as well, but it is going to be at the ultimate end state, the cost of doing business and indeed putting small businesses like mine out of that business completely.

Chairman SCHROCK. Legal costs could kill you.

Ms. GIORDANO. Exactly.

Chairman SCHROCK. Yes. Shane?

Mr. HAM. I agree with all of the other witnesses on this preemption thing, but I think probably even worse would be to implement a Do Not Spam list without the resources to do it correctly because

it could turn into a complete disaster if it is not done right, or it would probably involve a very complicated technical situation where the FTC has to set itself up as a remailer.

There are hurdles that need to be challenged, but if it is not done right then the spam problem will get worse literally within minutes after implementing—.

Chairman SCHROCK. So what I hear you saying is maybe a federal guideline would be more appropriate than California doing their thing, Utah doing their thing?

Mr. HAM. Definitely. Definitely.

Chairman SCHROCK. Okay. Wayne?

Mr. CREWS. Just be cautious about small business bearing the brunt of this. They will be the easy mark.

Chairman SCHROCK. They will be.

Mr. CREWS. I mean, it is the case that big companies have been targeted too by ambitious lawyers because they are easy to get to, and you cannot get to a lot of these bad guys.

Also watch out for loopholes. I mean, a lot of the reasons the spam you are getting has these random characters in it is because of the state laws that say you cannot send the same message to everybody. They shift it a little bit and send the stuff out anyway.

Whatever is done, it is not just preemption of the states. That does not concern me so much as preemption of what the market needs to do because ultimately the problem cannot be solved here. It is a technological, organizational industry problem that has to be solved that way, and it is not just spam. It is issues over cyber security and things of that sort that are even more fundamental than spam, but have to do with bad actors that you do not want getting onto your networks.

Also, another thing here. You asked about what is the worst you could do. You have to watch out for what liability provisions could emerge here. There was spam legislation last year and that had been debated this year that would give ISPs immunity from liability.

Now, I think negotiating something like that in the marketplace is perfectly appropriate, but if you have an evolving market where questions of who is liable if a message does not go through needs to be worked out through commerce, through the commercial process. It is inappropriate for Congress to stipulate that.

Similarly, in the House the spam legislation, of course, Zoe Lofgren's bill, for example, who did not want legislation a couple years ago, but now does. At that time she thought people could deal with it in a lot of ways, but the problem has gotten a lot worse.

She would set up a bounty for consumers to go after spam. Now, if I am a small business person I am terrified then because I am scared to use e-mail because I know how vindictive and malicious people can get sometimes. If they know that the law is going to let them sue \$500 for every unsolicited e-mail or something like that, I am not going to work anymore. I am just going to look for spams too and hope I get them.

You have to be careful. Spam is a huge problem, but, on the other hand, if it is a small business that has sent out an unsolicited e-mail, you know, the harm that they have caused is far less.

If you were talking about a legitimate company that is using its fax list or its members who bought its products and things, the harm caused by them sending out an e-mail is far below what some of those penalties could be.

Chairman SCHROCK. It seems like the greatest harm is the time and money it costs a company to address it. As Catherine said, she has a person and a half who has to address this. She has to pay them, and that is a cost she has. If some regulation was put in place, she might not have to.

Charlie?

Mr. GONZALEZ. I do have to comment on the private cause of action because I am still a believer that it is appropriate in certain circumstances.

I understand what you are saying. I think a lawyer that basically gets his staff together and says okay, let us make a list of all the things so we have a cause of action is deplorable. I think it is sanctionable and I think what is left of what used to be a great profession even further down.

What we are talking about is you have a remedy, and the consumer, the small business or whatever communicates to the sender. I am not on your list. I do not want to be on your list. I am rejecting it. You are ignored. Now, do you have to wait for the government to act on that? Do you really believe you are going to get your Attorney General or the appropriate agency or department of the United States Government to move quickly enough on this?

If they are doing it to you, they are doing it to thousands and thousands of other people, so I think it is appropriate that in certain circumstances, which is pretty outrageous, that the individual have that cause of action.

Now, what is a measure of damages? I think you are right. How is an individual harmed? Do you have groups, parties that come together for that purpose and go after the bad actors? I think there is a legitimate role for the private sector there because the profession, the private lawyer and the private practice is part of that private sector.

I do not want to dismiss that out of hand. I think it can be appropriate again in limited and very specific circumstances. I do appreciate what you are saying here on the abuses and the fact that I do not want a huge target being drawn on every small businessman and woman in this country by anybody who is litigious.

Thank you again for your concerns and your testimony this morning and afternoon.

Chairman SCHROCK. Let me just ask one final question. Do you have any comments on what Howard Beales talked about when he was here?

Mr. CERASALE. Well, I think Howard did talk about needing enforcement, needing funds for enforcement, and I think that that is very appropriate.

One of the things that he did say, however, was a difficulty in trying to find people. A lot of times if we are looking at really commercial stuff, the pornography stuff is more difficult, but to try to give funds to follow the money. Even though people can hide right now, if they are trying to sell something you can try to follow the money. That takes resources.

We understand, and it is hard for me to believe this figure, but from of the Federal Bureau of Investigation when we have been working with them trying to set up and get some people who are currently violating the law with spam, they said that really they think there are about between 150 and 300 really bad actors that produce most of the stuff.

Now, I do not know. It is hard for me to believe that, but that is what they have told us, and they have told others that. It may be that some funds to try, and I think Howard's thing was funds to give them enforcement authority to go after them now.

I mean, the saddest thing about this whole spam debate is that the FTC found that two-thirds on their face when they are looking at the spam study were fraudulent. AOL says that 90 percent that they receive are fraudulent. They are already violating laws, and we are not going to get them, which means that there is a real enforcement problem.

I think that that is someplace that Congress should look at very closely to see if we can get some funds into some enforcement to go get some of these people now.

Chairman SCHROCK. Did you say FBI?

Mr. CERASALE. FBI, yes.

Chairman SCHROCK. If they know it is that number, how do they know who it is? If they know who they are, why can they not stop it?

Mr. CERASALE. That is a good question that we have asked.

Chairman SCHROCK. Yes.

Mr. CERASALE. Now, we are working with them on a project called Slam Spam actually. The DMA is working with them. We are giving them some money to get some agents directly focused on spam because it is hard. It is intensive. It needs lots of resources, and it is not necessarily the glory arrest.

We would hope to get some arrests soon with some spammers, but I think that enforcement money is probably a good way to spend some resources because we can go get some people that are already breaking laws.

Chairman SCHROCK. Any others of you have comments on Howard?

[No response.]

Chairman SCHROCK. Let me join Mr. Gonzalez in saying thank you very much. You have been very patient. Your testimony and answers to questions have been very helpful.

I feel certain something very useful will come out of this and help you prevent the problems you have been having so that it will not happen again and again.

Thank you very much for being here. This hearing is adjourned.

[Whereupon, at 1:13 p.m. the Subcommittee was adjourned.]

Statement of Ed Schrock
Chairman
Subcommittee on Regulatory Reform and Oversight
Committee on Small Business
United States House of Representatives
Washington, DC
October 30, 2003

Good morning, ladies and gentlemen. Since the inception of the internet and electronic mail, businesses have found opportunities to use both as vehicles for marketing and advertising. Every day, Americans receive billions of e-mails, and its low cost allows marketers and businesspeople to reach wider audiences than ever before. Unfortunately, like any business practice in the United States, there are those who abuse this technology by sending bulk unsolicited e-mails to users without their permission. Spam, as it has been dubbed, is estimated to constitute over 40 percent of commercial e-mail. It clogs e-mail servers, reduces productivity, inhibits growth, and has a direct effect on small businesses in the United States. There are, however, many small businesses in the United States who execute e-mail marketing campaigns legally, and who use e-mail as a tool to inform and communicate with their customers.

Several current legislative proposals exist to combat spam. Options include increasing the jurisdiction of the Federal Trade Commission, creating a "do-not-e-mail" registry, requiring "opt-in" or "opt-out" provisions, requiring all bulk e-mailers to have trusted identification, or imposing harsher penalties on criminal spammers. Whatever the ultimate remedy, we want to make sure that the specific impacts on small businesses are taken into account. Over a million small businesses use e-mail as a marketing tool and

millions more use e-mail to communicate with employees, suppliers, and others critical to their business. Criminal spam cannot be allowed to prevent e-mail from its legitimate uses. And as time passes, the problem will only get worse if action is not taken.

Right now, I would like to thank our witnesses for coming in today. I look forward to all your testimony. We'll now have any additional opening statements.

35

PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION ON

“UNSOLICITED COMMERCIAL EMAIL”

Before the

COMMITTEE ON SMALL BUSINESS

SUBCOMMITTEE ON REGULATORY REFORM AND OVERSIGHT

U.S. HOUSE OF REPRESENTATIVES

Washington, D.C.

October 30, 2003

Mr. Chairman, the Federal Trade Commission appreciates this opportunity to provide information to the Subcommittee on the agency's efforts to address the problems that result from bulk unsolicited commercial email ("spam"), with particular focus on how spam affects small businesses. This statement discusses the Commission's law enforcement efforts against spam, describes our efforts to educate consumers and businesses about the problem of spam, and focuses particularly on the Commission's Spam Forum and several studies on the subject that the Commission's staff has undertaken in recent months. It also discusses legislative ideas to enhance the Commission's effectiveness in fighting spam.¹

As the federal government's principal consumer protection agency, the FTC's mission is to promote the efficient functioning of the marketplace by acting against unfair or deceptive acts or practices and increasing consumer choice by promoting vigorous competition. To fulfill this mission, the Commission enforces the Federal Trade Commission Act, which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.² Online commerce, including unsolicited commercial email, falls within the scope of this statutory mandate.

The problems caused by unsolicited commercial email go well beyond the annoyance spam causes to the public. Indeed, these problems include the fraudulent and deceptive content

¹ The views expressed in this statement represent the views of the Commission. My oral statements and responses to any questions you may have represent my own views, and not necessarily the views of the Commission or any other Commissioner.

² The FTC has limited or no jurisdiction over specified types of entities and activities. These include banks, savings associations, and federal credit unions; regulated common carriers; air carriers; non-retail sales of livestock and meat products under the Packers and Stockyards Act; certain activities of nonprofit corporations; and the business of insurance. *See, e.g.*, 15 U.S.C. §§ 44, 45, 46 (FTC Act); 15 U.S.C. § 21 (Clayton Act); 7 U.S.C. § 227 (Packers and Stockyards Act); 15 U.S.C. §§ 1011 *et seq.* (McCarran-Ferguson Act).

of most spam messages, the offensive content of many spam messages, the sheer volume of spam being sent across the Internet, and the security issues raised because spam can be used to disrupt service or as a vehicle for sending viruses.

FTC Spam Forum

Building upon our research, education, and law enforcement efforts, the FTC held a three-day public forum from April 30 to May 2, 2003 on spam email. This was a wide-ranging public examination of spam from all viewpoints. The Commission convened this event for two reasons. First, spam is frequently discussed, but facts about how it works, its origins, what incentives drive it, and so on, are not widely known. The Commission anticipated that the Forum would generate an exchange of useful information about spam to help inform the public policy debate. This could help the Commission determine what it might do to more effectively fulfill our consumer protection mission in this area. Second, the Commission sought to act as a potential catalyst for solutions to the spam problem. Through the Forum, the Commission brought to the table representatives from as many sides of the issue as possible to explore and encourage progress toward potential solutions to the detrimental effects of spam.

Virtually all of the panelists at the Commission's recent Spam Forum opined that the volume of unsolicited email is increasing exponentially and that we are at a "tipping point," requiring some action to avert deep erosion of public confidence that could hinder, or even destroy, email as a tool for communication and online commerce. In other words, as some have expressed it, spam is "killing the killer app." The consensus of all participants in the workshop was that a solution to the spam problem is critically important, but cannot be found overnight. There is no quick or simple "silver bullet." Rather, solutions must be pursued from many

directions – technological, legal, and consumer action. The Forum explored and helped to suggest paths to follow toward solving the spam problems. Such solutions will depend on cooperative efforts between government and the private sector.

Effect of Spam on Small Businesses

In addition to discussing potential solutions, panelists at the Forum also pointed to the damaging effect spam has on businesses, and particularly on small businesses. Although a single piece of spam to a single consumer causes *de minimis* economic harm, the cumulative economic damage from spam is enormous, and growing. There is a lack of empirical research regarding the costs of spam, but estimates have ranged from \$10 billion to \$87 billion a year.³

The flood of fraudulent and offensive spam robs businesses that would like to use commercial email messages as a low-cost way to market their goods and services. Legitimate sellers' messages tend to be drowned out or ignored by consumers who are inured to commercial email messages because so much spam is so distasteful.

A Forum panelist from Aristotle, a small Internet Service Provider ("ISP") located in Arkansas, stated that spam is its number one customer complaint and that addressing the increasing amount of spam is shaking the foundations of his small business. The panelist stated that in February 2002, spam made up 35 percent of its system, but currently 65 to 70 percent of

³ These estimates cover everything from the cost of anti-spam technology, such as filters, to the cost of lost worker productivity. See Saul Hansell, *Totaling Up the Bill for Spam*, N.Y. TIMES, July 28, 2003, § C, col. 2 (Late Edition):

Ferris Research, says the cost is \$10 billion in the United States this year. The Radicati Group estimates the worldwide cost at \$20.5 billion. Another firm, Nucleus Research, shoots higher. By its reckoning, the economic cost is \$874 a year for every office

the email on its system is spam. According to this panelist, Aristotle does not have the resources of large ISPs and that the increase in spam essentially means that this small business is fighting a “denial of service” attack every day: when Aristotle experiences a deluge of spam, its servers deliver email more slowly, customer complaints increase dramatically, and the customer support team struggles to keep up with the complaints.

Spammers’ practice of “harvesting”⁴ email addresses from public places on the Internet, such as websites, also poses particular harm to small businesses, as a principal means of communicating with customers for many small businesses often is through email addresses posted on the businesses’ websites. Commission staff conducted an examination of this practice in its “Spam Harvest,” in which we analyzed what online activities place consumers at risk for receiving spam. The examination discovered that one hundred percent of the email addresses posted in chat rooms received spam; one received spam only eight minutes after the address was posted. Eighty-six percent of the email addresses posted at Web pages and newsgroups received spam, as did 50 percent of addresses at free personal Web page services, 27 percent from message board postings, and 9 percent of email service directories. The “Spam Harvest” also found that the type of spam received was not related to the sites where the email addresses were posted.⁵

worker with an e-mail account, which multiplied by 100 million such workers amounts to about \$87 billion for the United States.

⁴ Email address harvesting is the practice of using computer programs to search public areas on the Internet to compute, capture, or otherwise “harvest” lists of email addresses. See <<http://www.ftc.gov/spam>>.

⁵ For example, email addresses posted to children's newsgroups received a large amount of adult-content and work-at-home spam.

As part of this project, the staff developed consumer education material, including a publication, "E-mail Address Harvesting: How Spammers Reap What You Sow," that provides tips, based on the lessons learned from the Spam Harvest, to Internet users who want to minimize their risk of receiving spam. The tips advise, among other things, that consumers can minimize the chances of their addresses being harvested by using at least two email addresses--one for use on websites, newsgroups and other public venues on the web, and another email address solely for personal communication. Another suggested strategy to reduce spam is "masking" (disguising) email addresses posted in public. Masking involves putting a word or phrase in one's email address so that it will trick a harvesting computer program, but not a person. For example, if one's email address is "johndoe@myisp.com., one could mask it as "johndoe@spamaway.myisp.com." ⁶ In addition, a Spam Forum panelist from the Center for Democracy and Technology also noted that currently there are available techniques to publicly post addresses on websites in ways that are not readily interpreted by computers as being email addresses, thus preventing the addresses from being harvested.⁷

Law Enforcement

The Forum is only the most recent example of the FTC's role as convener, facilitator, and catalyst to encourage government and private sector action to address the problems caused by spam. But the Commission also plays another important role – that of law enforcer. For example, the Commission has pursued a vigorous law enforcement program against deceptive spam, and to date has brought 55 cases in which spam was an integral element of the alleged

⁶ Nevertheless, some harvesting programs may be able to pick out common masks.

⁷ For more information on these techniques, *see* <http://www.cdt.org/resourcelibrary/Spam/Tools/>.

overall deceptive or unfair practice. Most of those cases focused on the deceptive content of the spam message, alleging that the various defendants violated Section 5 of the FTC Act through misrepresentations in the body of the message.⁸ More recently, the Commission has expanded the scope of its allegations to encompass not just the content of the spam but also the *manner* in which the spam is sent. Thus, *FTC v. G. M. Funding*⁹ and *FTC v. Brian Westby*¹⁰ allege (1) that email “spoofing” is an unfair practice,¹¹ and (2) that failure to honor a “remove me” representation is a deceptive practice. In each of these cases, the defendants’ email removal mechanisms did not work and consumers’ emailed attempts to remove themselves from defendants’ distribution lists were returned as undeliverable.

Westby is also the first FTC case to allege that a misleading subject line is deceptive because it tricks consumers into opening messages they otherwise would not open. In other cases, the Commission has alleged that the defendants falsely represented that subscribing to defendants’ service could stop spam from other sources¹² or that purchasers of a spamming business opportunity could make substantial profits.¹³

⁸ E.g., *FTC v. 30 Minute Mortgage, Inc.*, No. 03-60021 (S.D. Fla. filed Jan. 9, 2003).

⁹ No. SACV 02-1026 DOC (C.D. Cal. filed Nov. 2002).

¹⁰ No. 032-3030 (N.D. Ill. filed Apr. 15, 2003).

¹¹ “Spoofing” involves forging the “from” or “reply to” lines in an email to make it appear that the email was sent from an innocent third-party. The third-party then receives bounced-back undeliverable messages and angry “do not spam me” complaints.

¹² *FTC v. NetSource One*, No. 022-3077 (W.D. Ky. filed Nov. 2, 2002).

¹³ *FTC v. Cyber Data*, No. CV 02-2120 LKK (E.D. Cal. filed Oct. 2002); *FTC v. Internet Specialists*, No. 302 CV 01722 RNC (D. Conn. filed Oct. 2002)

In May 2003, the FTC joined the Securities and Exchange Commission, United States Postal Inspection Service, three United States Attorneys, four state attorneys general, and two state regulatory agencies to file 45 criminal and civil law enforcement actions against Internet scammers.¹⁴ As part of this sweep, the FTC brought five federal court actions alleging the deceptive use of spam. In one case, the defendants allegedly used spam with deceptive representations that the email came from well-known entities, such as Hotmail or MSN, to market a "100% Legal and Legitimate" work-at-home opportunity. According to the complaint, although the spam promised consumers they could earn as much as \$1,500 a week stuffing envelopes supplied by the defendants, consumers ended up paying \$50 for a set of instructions on how to market a deceptive credit-repair manual.¹⁵ In another case, the defendant allegedly used spam to make false and deceptive income claims for a chain-letter scheme dubbed "Instant Internet Empire."¹⁶ A third complaint alleged that defendants used deceptive spam to market an advance-fee credit card scam.¹⁷ In each of these cases, the FTC was able to obtain preliminary injunctive relief and to shut down the operations.¹⁸

¹⁴ FTC Press Release, *Law Enforcement Posse Tackles Internet Scammers, Deceptive Spammers* (May 15, 2003), available at <<http://www.ftc.gov/opa/2003/05/swnetforce.htm>>.

¹⁵ *FTC v. Patrick Cella et al.*, No. CV-03-3202 (C.D. Cal.) (complaint filed May 7, 2003), available at <<http://www.ftc.gov/os/2003/05/patrickcellacmp.pdf>>.

¹⁶ *FTC v. K4 Global Publishing, Inc. et al.*, No. 5:03-CV0140-3 (M.D. Ga.) (complaint filed May 7, 2003), available at <<http://www.ftc.gov/os/2003/05/k4globalcmp.pdf>>.

¹⁷ *FTC v. Clickformail.com, Inc.*, No. 03-C-3033 (N.D. Ill.) (complaint filed May 7, 2003), available at <<http://www.ftc.gov/os/2003/05/clickformailcmp.pdf>>.

¹⁸ In the other two cases, the FTC filed stipulated final orders prohibiting future participation in email chain letters. *FTC v. Evans*, No. 4:03CV178 (E.D. Tex.) (complaint and stipulated final judgment filed May 9, 2003); *FTC v. Benson*, No. 03CV0951 (N.D. Tex.)

In addition to the law enforcement actions, in this sweep, the FTC and 17 other federal and state consumer protection and law enforcement agencies initiated an effort to reduce deceptive spam by urging organizations to close "open relays."¹⁹ Fifty law enforcers from 17 agencies identified 1,000 potential open relays, 90 percent of which were in 16 countries: U.S., China, Korea, Japan, Italy, Poland, Brazil, Germany, Taiwan, Mexico, Great Britain, Chile, France, Argentina, India, Spain, and Canada. The agencies drafted a letter, translated into 11 languages and signed by 14 different U.S. and international agencies, urging the organizations to close their open relays to help reduce spam.

Most recently, the Commission has tackled the problem of "phishing," which is the practice of using hijacked corporate logos and deceptive spam to con consumers out of credit card numbers and other financial data.²⁰

As these law enforcement actions demonstrate, the Commission has attacked and will continue to attack deception and unfairness in every aspect of spam.

(complaint and stipulated final judgment filed May 6, 2003). Both are available at <<http://www.ftc.gov/opa/2003/05/swnetforce.htm>>.

¹⁹ An open relay is an email server that is configured to accept and transfer email on behalf of any user anywhere, including unrelated third parties, which allows spammers to route their email through servers of other organizations, disguising the origin of the email. Open proxies are a related aspect of the problem. An open proxy is a mis-configured proxy server through which an unauthorized user can connect to the Internet. Spammers use open proxies to send spam from the computer network's ISP or to find an open relay. See FTC Facts for Business, *Open Relays – Close the Door on Spam* (May 2003), available at <<http://www.ftc.gov/bcp/online/pubs/buspubs/openrelay.htm>>.

²⁰ *FTC v. Unnamed Minor Defendant*, No. 03-5275 (C.D. Cal.) (complaint filed July 21, 2003), available at <<http://www.ftc.gov/opa/2003/07/phishing.htm>>.

Approaches to Solving the Spam Problem

Solutions to the problems posed by spam will not be quick or easy; nor is one single approach likely to provide a cure. Instead, a balanced blend of technological fixes, business and consumer education, legislation, and enforcement will be required. Technology that empowers consumers in an easy-to-use manner is essential to getting immediate results for a number of frustrated end-users. Any solution to the problems caused by spam should contain the following elements:

1. Enhanced enforcement tools to combat fraud and deception;
2. Support for the development and deployment of technological tools to fight spam;
3. Enhanced business and consumer education; and
4. The study of business methods to reduce the volume of spam.

The Commission's legislative recommendations, discussed below, would enhance the agency's enforcement tools for fighting spam. In addition, the FTC, through a recently-created Federal/State Spam Task Force, will continue pursuing vigorous law enforcement, reaching out to key law enforcement partners, and strengthening cooperation with criminal authorities. The Task Force is designed to help to overcome some of the obstacles that spam prosecutions present to law enforcement authorities.

The Commission's experience shows that the primary law enforcement challenges are to identify and locate the targeted spammer. Of course, finding the wrongdoers is an important aspect of all law enforcement actions, but in spam cases it is a particularly daunting task. Spammers can easily hide their identity, falsify the electronic path of their email messages, or send their messages from anywhere in the world to anyone in the world. Tracking down a

targeted spammer typically requires an unusually large commitment of staff time and resources, and rarely can it be known in advance whether the target's operation is large enough or injurious enough to consumers to justify the resource commitment. For example, in some instances, state agencies spent considerable front-end investigative resources to find a spammer, only to discover at the back end that the spammer was located outside the state's jurisdiction. State and federal agencies recognize the need to share the information obtained in investigations, so that the agency best placed to pursue the spammer can do so more efficiently and quickly. The Task Force should facilitate this process. Further, it can serve as a forum to apprise participating agencies of the latest spamming technology, spammer ploys, and investigational techniques.

Through the Task Force, the FTC will reach out not only to its civil law enforcement counterparts on the state level, but also to federal and state criminal authorities. Although few criminal prosecutions involving spam have occurred to date,²¹ criminal prosecution may well be appropriate for the most egregious conduct. The FTC and its partners in criminal law enforcement agencies continue to work to assess existing barriers to successful criminal prosecutions. The FTC will explore whether increased coordination and cooperation with criminal authorities would be helpful in stopping the worst actors.

Improved technological tools will be an essential part of any solution as well. A great deal of spam is virtually untraceable, and an increasing amount crosses international boundaries. Panelists estimated that from 50 percent to 90 percent of email is untraceable, either because it

²¹ See, e.g., *United States v. Barrero*, Crim. No. 03-30102-01 DRH (S.D. Ill. 2003) (guilty plea entered May 12, 2003). Like the related case, *FTC v. Stuffingforcash.com Corp.*, Civ. Action No. 02 C 5022 (N.D. Ill. Jan. 30, 2003), the allegations in this criminal prosecution were based on fraud in the seller's underlying business transaction.

contains falsified routing information or because it comes through open relays or open proxies.²² Because so much spam is untraceable, technological development will be an important element in solving spam problems. To this end, the FTC will continue to encourage industry to meet this challenge.

Action by businesses and consumers who may receive spam will be a crucial part of any solution to the problems caused by spam. A key component of the FTC's efforts against spam is educating recipients of spam about the steps they can take to decrease the volume of spam they receive.²³

Finally, several initiatives for reducing the overwhelming volume of spam were discussed at the FTC's Spam Forum. At this point, questions remain about the feasibility and likely effectiveness of these initiatives. The FTC intends to continue its active role as catalyst and monitor of technological innovation and business approaches to addressing spam.

²² Brightmail recently estimated that 90% of the email that it analyzed was untraceable. Two panelists at the Commission's Spam Forum estimated that 40% to 50% of the email it analyzed came through open relays or open proxies, making it virtually impossible to trace. Even when spam cannot be traced technologically, however, enforcement is possible. In some cases, the FTC has followed the money trail to pursue sellers who use spam. The process is resource intensive, frequently requiring a series of ten or more CIDs to identify and locate the seller in the real world. Moreover, the seller and the spammer often are different entities. In numerous instances, FTC staff cannot initially identify or locate the spammer and can only identify and locate the seller. In many of those cases, in the course of prosecuting the seller, staff has, through discovery, sought information about the spammer who actually sent the messages. This, too, involves resource-intensive discovery efforts.

²³ The FTC's educational materials provide guidance on how to decrease the chances of having an email address harvested and used for spam, and suggest several other steps to decrease the amount of spam an address may receive. The FTC's educational materials on spam are available on the FTC website. See <<http://www.ftc.gov/spam>>.

Legislation to Enhance the FTC's Effectiveness To Fight Fraudulent Spam

Effective spam legislation must address the following three issues: First, legislation must address how to find the person sending the spam messages. Although we believe that technological changes will most effectively resolve this issue, we have proposed several procedural legislative changes that can provide some assistance in our law enforcement investigations. Second, legislation must deal with how to deter the person sending the spam messages. As discussed below, the Commission believes that civil penalties, and possibly criminal sanctions, would help address this issue. Finally, legislation must determine what standards will govern non-deceptive, unsolicited commercial email. The Commission believes that the appropriate standards would include clear identification of the sender of a message and by empowering consumers to end the flow of messages that they do not wish to receive.

It would be useful to have additional authority, addressing both procedural and substantive issues, that would enhance the agency's effectiveness in fighting fraud and deception. The procedural legislative proposals would improve the FTC's ability to investigate possible spam targets, and the substantive legislative proposals would improve the agency's ability to sue these targets successfully, including increased penalties for violations.

Procedural Proposals

The FTC's law enforcement experience shows that the path from a fraudulent spammer to a consumer's in-box frequently crosses at least one international border and often several. Thus, fraudulent spam exemplifies the growing problem of cross-border fraud. Two of the provisions in the Commission's proposed cross-border fraud legislation, discussed at the recent reauthorization testimony, would be particularly helpful to enable the FTC to investigate

deceptive spammers more effectively and work better with international law enforcement partners.

First, the Commission has asked Congress to amend the FTC Act to allow FTC attorneys to seek a court order requiring a recipient of a Civil Investigative Demand (“CID”) to maintain the confidentiality of the CID for a limited period of time. Several third parties have told us that they will provide notice to the target before they will share information with us, sometimes because they believe notice may be required and sometimes even if such notice clearly is not required by law.

Second, the Commission asked Congress to amend the FTC Act so that FTC attorneys may seek a court order temporarily delaying notice to an investigative target of a CID issued to a third party in specified circumstances. Currently, the Right to Financial Privacy Act (“RFPA”) and the Electronic Communications Privacy Act (“ECPA”) require such notice.

The FTC’s experience is that fraud targets often destroy documents or hide assets when they receive notice of FTC investigations. Although the RFPA and ECPA provide a mechanism for delaying notice, the FTC’s ability to investigate would be improved by tailoring the bases for a court-ordered delay more specifically to the types of difficulties the FTC encounters, such as transfers of assets offshore. In addition, it is unclear whether FTC attorneys can file such applications, or whether the Commission must seek the assistance of the Department of Justice. Explicit authority for the FTC, by its own attorneys, to file such applications would streamline the agency’s investigations of purveyors of fraud on the Internet, ensuring that the agency can rapidly pursue investigative leads.

Other legislative proposals would enhance the FTC's ability to track deceptive spammers. First, we request that the ECPA be clarified to allow the FTC to obtain complaints received by an ISP regarding a subscriber. Frequently, spam recipients complain first to their ISPs, and access to the information in those complaints would help the agency to determine the nature and scope of the spammer's potential law violations, as well as lead the agency to potential witnesses.

Second, we request that the scope of the ECPA be clarified so that a hacker or a spammer who has hijacked a bona fide customer's email account is deemed a mere unauthorized user of the account, not a "customer" entitled to the protections afforded by the statute. Because of the lack of a statutory definition for the term "customer," the current statutory language may cover hackers or spammers. Such a reading of the ECPA would permit the FTC to obtain only limited information about a hacker or spammer targeted in an investigation. Clarification to eliminate such a reading would be very helpful.

Third, we request that the ECPA be amended to include the term "discovery subpoena" in the language of 18 U.S.C. § 2703. This change is particularly important because a district court has ruled that the FTC staff cannot obtain information under the ECPA from ISPs during the discovery phase of a case, which limits the agency's ability to investigate spammers.²⁴

Substantive Proposals

Substantive legislative changes also could aid in the FTC's law enforcement efforts against spam. Although Section 5 of the FTC Act provides a firm footing for spam prosecutions, additional law enforcement tools could make more explicit the boundaries of legal and illegal conduct, and they could enhance the sanctions that the agency can impose on violators.

²⁴ See *FTC v. Netscape Comm. Corp.*, 196 F.R.D. 559 (N.D. Cal. 2000).

First, any legislation should give the FTC some authority via rulemaking to address deceptive practices relating to spam. Agency rules could be adapted to new changes in technology without hindering technological innovation, thus providing the market with direction, but doing so within a framework that could change as the problems evolve. Whether addressed through the legislation itself or through rulemaking, unlawful practices that should be prohibited include: using false header or routing information; using false representations in the “subject” line; using false claims that an unsolicited commercial email message was solicited; using false representations that an opt-out request will be honored; sending any recipient a commercial email message after such recipient has requested not to receive such commercial email messages; failing to provide a reasonable means to “opt out” of receiving future email messages; and sending commercial email to an address obtained through harvesting or a dictionary attack. Moreover, any statute also should prohibit assisting and facilitating any of the above, *i.e.*, providing substantial assistance to another party engaged in any violation knowing or consciously avoiding knowing that such party is engaged in such violation.

Second, any legislation should embody the same standard of liability that is embodied in Section 5 of the FTC Act, without a general requirement to show intent or knowledge. Imposition of intent or knowledge requirements as a precondition of liability would actually make the FTC’s ability to enforce the specific anti-spam statute more restrictive than the agency’s existing authority under Section 5 to attack spam and would unnecessarily complicate enforcement.

Third, any statute or rule issued under the statute should be enforceable by the FTC like other FTC rules. This entails actions in federal district court, authority to seek preliminary and

permanent injunctions and other equitable relief, and liability for civil penalties of up to \$11,000 per violation. (The amount of civil penalties is governed by statutory factors, such as ability to pay, previous history of such conduct, egregiousness of the conduct, etc.).

Fourth, any legislation should authorize states to enforce the statute or FTC rule in federal court. A state enforcement mechanism has proven successful in other areas of consumer protection, such as telemarketing, and would make the states more capable law enforcement partners with the Commission.

Finally, any statute should seek to assure consistency between state and federal laws. The scope of the Internet and of email communication is global, transcending national boundaries. Congress should seek to minimize artificial barriers that would break up this market.

Additionally, the criminalization of false header and routing information should be explored. The FTC staff has been discussing with criminal authorities the likely effect of a specific statute that criminalized this conduct.²⁵

Admittedly, we recognize that these legal steps alone will not solve the growing spam problem. Nor is it clear what impact these steps will have on some of the other problems associated with spam (*e.g.*, security). These issues may need to be addressed separately. Nevertheless, the FTC believes that legislation, such as that described above, would provide more effective investigative and enforcement tools and would enhance the FTC's continuing law enforcement efforts.

²⁵ Any legislation that criminalizes certain types of spam activities should not negatively impact the FTC's existing Section 5 authority or impose new standards of proof, scienter, or evidence for civil enforcement cases.

Conclusion

Email provides enormous benefits, as a communication tool, to consumers and businesses, including small businesses. The increasing volume of spam to ISPs, to businesses, and to consumers, coupled with the widespread use of spam as a means to perpetrate fraud and deception, put these benefits at serious risk. The Commission looks forward to continuing its research, education, and law enforcement efforts to protect consumers and businesses from the current onslaught of unwanted messages.

The Commission appreciates this opportunity to describe its efforts to address the problem of spam.

53

TESTIMONY OF

JERRY CERASALE

ON BEHALF OF THE DIRECT MARKETING ASSOCIATION

BEFORE THE SUBCOMMITTEE ON REGULATORY REFORM AND OVERSIGHT

COMMITTEE ON SMALL BUSINESS

THE UNITED STATES HOUSE OF REPRESENTATIVES

October 30, 2003

Good morning, Mr. Chairman and members of the Subcommittee. I thank you for the opportunity to appear before you as you investigate the vital role played by legitimate commercial e-mail in the business models of small and medium-sized enterprises. I am Jerry Cerasale, Senior Vice President for The Direct Marketing Association, Inc. ("The DMA").

The DMA is the largest trade association for businesses interested in direct, database, and interactive marketing and electronic commerce. The DMA represents more than 4,500 companies in the United States and 54 foreign nations. Founded in 1917, its members include direct marketers from 50 different industry segments, as well as the non-profit sector. Included are catalogers, financial services, book and magazine publishers, retail stores, industrial manufacturers, Internet-based businesses, and a host of other segments, as well as the service industries that support them. The majority of direct marketers are small businesses. In our catalog segment alone, for example, according to Dun and Bradstreet, over 17,000 of the 21,000 catalog companies in the United States have annual sales of less than \$1,000,000.

E-commerce offers a huge promise to all companies, large and small, to reach out to a global marketplace at reasonable costs, and e-mail is an important cog in that promise. Unfortunately, e-commerce also is a means to fill electronic mailboxes, at homes and businesses, and swamp Internet service providers with untargeted offers, fraudulent offers, pornography and computer viruses. Thus, I appear before you today on behalf of businesses, large and small, to ask that Congress move vigorously against the fraudulent spam that is plaguing consumers' in-boxes, while at the same time preserving the promise of an emerging dynamic, entrepreneurial marketplace created by commercial e-mail. From an economic point of view, legitimate commercial e-mail, whether sent to customers or prospects, is alive, well, and a vital part of the business model for businesses, particularly small and medium sized firms.

With the proliferation of web sites on the Internet, businesses have begun to pay for prominent placement of their information in any search engine inquiry. Small- and medium-sized businesses, therefore, are not prominent in Internet searches for products. Therefore, like so many entrepreneurs who grew their businesses in the days before the Internet, today's enterprises recognize that even in the on-line environment, customers must be actively acquired. Traditionally, this is a two step process: it means targeting a carefully selected list of prospective customers; then reaching out to such customers by using the most cost-effective means possible.

The Internet has dramatically reduced the cost of contacting such customers through to legitimate commercial email. Where sending prospecting letters via postal mail or hiring a sales force may cost thousands, even millions of dollars, e-mail may be sent for a fraction of the cost.

As a result, opportunities abound for small entrepreneurs seeking to win customers. These low barriers to customer acquisition offer newer or improved products, lower prices, and increased savings to customers who are willing to open up legitimate email from new firms of which they may have never heard. Competition will grow. It would be hard to imagine catalog companies growing to their present stature without nation-wide delivery of their catalogs in years gone by. Similarly, commercial e-mail may deliver economic growth and employment for businesses in the years and decades ahead.

Let me describe the current state of play of this marketplace. Based on the latest US Census Bureau data, DMA research estimates that already some 12% of the current \$138 billion Internet commerce marketplace is driven by commercial email. This translates into a minimum \$17.5 billion spent in response to commercial emails in 2003 -- purchases that include airline tickets and other forms of travel, entertainment, books, clothing, and so on, all from reputable companies.

TABLE 1. Value Of Internet And Commercial E-Mail Sales

	\$
Total U.S. Internet Commerce (1) (\$ Billions)	138.2
E-mail Sales as % Interactive Sales (2)	12.7%
Value of E-mail Sales (\$ Billions)	\$ 17.5

(SOURCE: (1) U.S. CENSUS BUREAU; (2) 2002 DMA STATE OF E-COMMERCE INDUSTRY REPORT)

Consumers recognize the value of commercial e-mail, and respond to both prospecting and customer-retention e-mail. When asked in May of 2003 by an independent polling organization in a nation-wide, statistically projectible survey, some 36% of adult American email users acknowledged buying one or more products or services in response to a legitimate commercial email solicitation. This translates into some 45 million Americans. Almost a quarter of these e-mail consumers, or about 11 million adult Americans, acknowledged purchasing in response to an unsolicited commercial email, or what our industry refers to as a solicitation to a prospect. Fully 72% of such survey respondents indicated their purchase from an unsolicited commercial email represented a cost savings, an even higher percentage than those who purchased in response to a commercial email from a company with whom they had previously done business.

TABLE 2. Consumer Expenditure On Solicited And Prospecting E-mail: Most Recent Purchase Within Last 12 Months

	COMMERCIAL E-MAIL TYPE		
	CUSTOMER	PROSPECTING	TOTAL
% ADULT E-MAIL USERS PURCHASING IN RESPONSE TO TYPE OF COMMERCIAL E-MAIL within 12 MOS. (3)	27%	9%	36%
ADULTS WITH E-MAIL PURCHASE within 12 MOS. (MILLIONS)	34.4	11.4	45.8
AVERAGE COST/MOST RECENT E-MAIL PURCHASE (3)	\$178	\$139	\$168
TOTAL EXPENDITURE/MOST RECENT E-MAIL PURCHASE (\$ MILLIONS)	\$6,109.8	\$1,584.6	\$7,694.4
% EMAIL CUSTOMERS REPORTING SAVINGS (3)	68%	72%	69%
ADULT EMAIL PURCHASERS REPORTING SAVINGS (MILLIONS)	23.4	8.2	31.6
AVERAGE SAVED PER RECENT E-MAIL PURCHASE (3)	\$52	\$38	\$48
TOTAL SAVINGS/MOST RECENT E-MAIL PURCHASE (\$ MILLIONS)	\$1,204.9	\$311.9	\$1,516.9

(SOURCE: (3) ORC INTERNATIONAL SURVEY, MAY 2003.)

The value of legitimate commercial email purchases by consumers now exceeds \$1.5 billion for prospecting email, and \$6.1 billion for customer-retention email, for a total of over \$7.6 billion spent by consumers alone.

Within this large and rapidly growing legitimate commercial email marketplace, small businesses are especially reliant on email marketing as one of the least expensive ways to acquire new customers and break into a marketplace that is dominated by large, traditional corporate entities.

The DMA routinely surveys its members to assess their usage of different marketing channels. In our most recent 2002 studies, we found that some 28% of small businesses did NOT have an in-house email list of customers –they were about 50% more likely to lack such a customer base of email contacts. This means that they are much more dependent than are large businesses on being able to email to other people’s customers, if they are to grow their enterprises. You can see that a legally required “opt-in” e-mail regime would disproportionately affect small business.

Table 3. Use of E-mail by Size of Company (Source: 2002 DMA STATE OF E-COMMERCE INDUSTRY REPORT)

	SMALL	MEDIUM	LARGE
Do not have an in-house e-mail list	28%	24%	20%
Have an in-house e-mail lists	72%	76%	80%

Furthermore, small enterprises told our research department in 2002 that over 21% of their total Internet marketing budget was devoted to e-mail campaigns. This compares to some 13% for large businesses, and only 6.2% for medium-sized businesses.

Table 4. Percentage of Total Marketing Budget Used for E-mail by Size of Company

	SMALL	MEDIUM	LARGE
Average	21.4%	6.2%	13.7%

(Source: 2002 DMA STATE OF E-COMMERCE INDUSTRY REPORT)

This reliance on email marketing by small or start-up businesses correlates strongly with the respective sales performance over the Internet by small, medium, and large businesses. Whereas the industry-wide average is some 12.7% of Internet-based sales being derived from e-mail, small businesses derive almost twice as much -- 21.4% -- of their Internet-based revenues from email promotions. And, as we have seen, a much larger proportion of such email promotions from small businesses are likely to be to prospects rather than to established customers. Moreover, small businesses reported that 2002 email-driven sales were increasing at a whopping 23% per year, at a time when the sales through other channels, or by other firms elsewhere in the economy, were either flat or growing slowly.

Table 5. Percentage of Internet Sales Derived From E-mail Based Promotions by Size of Company

	SMALL	MEDIUM	LARGE	TOTAL
Average	21.4%	7.0%	13.4%	12.7%

An example can help bring these statistics to life. According to a 2000 study commissioned by the Federal Small Business Administration, FTD.com represents an excellent example of the cost-savings email marketing represents. FTD.com reported profits of \$253,000 on revenues of \$18.2 million for the third quarter of 2000. What significantly contributed to that success, according to the study, was moving from print and TV advertising to direct marketing-- particularly e-mail marketing. This reduced customer acquisition costs from \$36 to \$17. This 50% reduction in reaching out to new customers contributed substantially to FTD's gross profit margins of 31 percent at a time when many other Internet-based firms were closing their shutters.

The online marketplace is critical for small businesses to find customers in a national, if not global, marketplace. Struggling start-ups or mom and pop operations see commercial email as an unprecedented, low-cost opportunity to entice potential customers who were previously beyond their grasp. They need to send email—not just to customers but also to prospects, who do not even know the company's name, in the hopes of having them become customers.

There should be no doubt that businesses that depend on prospecting e-mail abhor the illegitimate, offensive, and deceptive spam that is now clogging inboxes. This type of email is not what the vast majority of small businesses do. This fraudulent spam is the bane of their existence. It clogs their servers as much as it clogs yours or mine. It destroys the willingness that consumers otherwise might have to open up an unexpected email that might contain an attractive offer for a good or service from a company the consumer did not previously know about. This reduces response rates for small businesses, and does neither the small entrepreneur, nor the consumer, nor the U.S. economy as a whole, any good.

Legitimate direct marketers, especially from within the community of small business, are here to implore that Congress take all appropriate steps to rid our inboxes of fraudulent and offensive spam, while preserving the right of start-up enterprises and mom-and-pop Internet firms to grow their business by reaching out and acquiring new customers *via* prospecting email.

Thank you.

Bruce Goldberg
Weathermen Music
3331 Towerwood 305
Dallas, Tx 75234

My name is Bruce Goldberg from Weathermen Music of Dallas Texas. I am here to represent my business, but more importantly, I am here to represent all the small businesses in the United States that are powerless against unsolicited email.

In college I studied Business Marketing with the hopes that someday I would be able to work for myself and own my own business. After college I worked my way up the ladder for Neiman Marcus, completing their executive development program and working as part of their buying staff.

I have always had a passion for music. My passion soon turned into a hobby and I started buying and selling records at a monthly music convention. I started to keep a list of names and addresses of those who wanted to receive notification when I got new items. Before I knew it, I was mailing out 500 lists a week. I reinvested every dime I made and started to expand into music t-shirts. I put together a small mail order catalog, and before too long I was sending out more than 1,000 copies a month via U.S. mail. Around the same time, I started to subscribe to a service that would allow me to communicate with other people all over the world via the computer called "prodigy". Soon I was able to set up a tiny web page with a template on Prodigy. This was the beginning of my online company.

As my customer base grew, I decided to leave Neiman's to concentrate on my mail order company. When domain names were first being offered, I quickly bought the name "The Weathermen" as my company name with the marketing idea of being a "music forecaster". I invited my new customers to sign up for my free email updates. My list quickly grew from the initial 1,000 to 60,000. Today Weathermen Music is one of the largest online t-shirt music stores with over 50,000 regular worldwide customers and 6,000 web sites linked to the site. We carry about 4,000 different music t-shirts from all over the world. We are still considered a small business with only a handful of employees.

95% of all our sales and communication are done over the Internet. When I first started it never crossed my mind that I could even get an email that was bulk emailed to me about viagra, lowering my mortgage payment, losing weight or getting rid of my debt. Throughout the years, I started getting more and more spam but was pretty much able to control it by simply deleting it as it arrived. As my online presence grew, so did the amount of spam I received. I was finding that whereas most people would get 1 of each spam we were getting 5-10 of each, depending on how many of our email addresses were hit. The hard part was distinguishing the legitimate email from junk, as I have to treat each new email as a potential customer. A lot of legitimate emails were being accidentally deleted. Even as careful as I was, I would still lose customers by accidentally deleting

their messages. We were getting 15 spam emails to every 1 legitimate email. I needed to do something about this as it was getting increasingly worse. On more than one occasion, my company's server was so overloaded by spam, it shut itself down for several hours costing me a day's business and customers.

The first thing I did was to set up my account so that anything intended for ex- employees went right into the trash bin. The second thing I did was employ a spam filtering service that, would filter out any email that was previously reported by a fellow member as spam and put it into a separate "spam holding tank" for spam email. But the problem with this service is, however, is that sometimes it accidentally grabs legitimate email. In an average day, the spam mail folder will keep 1,000 spam emails from reaching our system. Today, even with all the filtering systems in effect, we still get three spam mails for every 1 legitimate email. I spend at least one hour a day sending spam to my trash box. I get spam 24 hours a day, 7 days a week. I was recently featured in an article in the Wall Street Journal about spam. Because of the article, I got spammed. I will probably get spammed from this testimony finding its way to the Internet. Instead of spending my time dealing with my mail situation, I could use the time to better serve my customers, increasing my profits, which in turn would generate more tax dollars for my community.

I believe something must be done about this situation that gets worse by the day. If the problem continues to grow at the rate it currently is growing it will be impossible for businesses to rely on the Internet and email as a means of communication. I believe people that send spam or harvest and sell email addresses should be fined and prosecuted. I believe that our government should try to work with other governments to abolish spam sent from other countries that try to prey on the elderly and the young by means of deception. I use email as my main form of communication. Imagine if you used the telephone as a main form of communication and your phone rang all day long with solicitors, but you had to answer every call to see who it was before you could hang up because you were afraid you would lose legitimate customers. Imagine, instead of spending your time before your hearings to make sure you were prepared to serve your community, you had to take that hour to weed through thousands of emails to find the ones you needed to start your work day. That's what I do every day. I also believe that if lawmakers were the targets of the same amount of deceptive and unwanted spam as small businesses and had to go through all the mail themselves as a lot of small businesses do, spam would of already have been outlawed.

I love my country. I grew my business from the ground up by using simple principles that consisted of good communication and providing a fair- priced good quality product to people who normally would not be able to find it. You could say that spam finally shut me down. This past week I sold my company and am currently unemployed. For the sake of the new owner, I hope that this testimony will help result in a resolution of the end of deceptive, unwanted, unsolicited commercial email. I hope whatever career I travel down next, I do not have to put up with the same frustration that plagued me and other small businessmen for years.

Thank you for listening.

61

Testimony

for

**United States House of Representatives
Committee on Small Business
Subcommittee on Regulatory Reform and Oversight**

Hearing on Spam and its Effects on Small Business

by

**John A. Rizzi
President and Chief Executive Officer
e-Dialog, Inc.**

October 30, 2003

Executive Summary

e-Dialog is a small business of 51 people, located in Lexington, Massachusetts, with small offices in Los Angeles and London. This business is 100 percent dependant on e-mail being an effective marketing and communications channel. We are an e-mail service provider. Simply, our mission is to help large organizations do e-mail right. We work with industry leading companies helping them use e-mail as an effective relationship tool with their customers. We are extremely pleased that so much activity is happening at the legislative level to bring about an end to spam.

It is not over-dramatic to say that spam has reached epidemic proportions. The well-published pains and costs to both businesses and consumers are staggering. They can not be denied. The justifiable outcry, however, has over shadowed the good side of e-mail, and especially how it is helping small businesses to succeed. These benefits need to be understood and small businesses need to be protected so they can continue to capitalize on this inexpensive and effective communication channel with their customers.

Small businesses are not perpetrators of spam, they are victims. Their valuable messages are lost in the cluttered mailboxes of their recipients, or are blocked indiscriminately by ISPs and mail filters so they never reach the intended recipient. This is not only bad for the business person, but it may generate bad will with her customer who doesn't receive a valuable notice or communication. Meanwhile, the small business owner is very interested in doing e-mail right and not breaking any laws. Unfortunately the tangled web of duplicative and inconsistent state laws is impossible for a small business owner to understand and adopt, leaving himself exposed every time he pushes the send button. To help this person we need a single, preemptive federal law that can be adopted broadly.

The worst kind of spam comes from bad people mostly uninterested in laws. This creates a conundrum since the intention of any new law is to stop spam. Unfortunately these bad actors can hide on the internet and never have to answer to a magistrate. Ultimately these spammers can only be stopped with technology that removes their anonymity. Once they

can be identified, the law can do its job. Fortunately there are several industry initiatives developing promising technology that will require authentication of the sender of all volume e-mail transmissions. These initiatives are moving along quickly and will be an essential part of solving the spam problem. Development of effective technology must be supported at every level.

One popular initiative under consideration is the creation of a national Do-Not-E-mail (DNE) registry. While intuitively this sounds reasonable, once you look at it carefully it is more likely a disaster waiting to happen, especially for small businesses. The security of the list would always be challenged (a hack *will* happen sooner or later), the adoption costs for small businesses would be significant, and the end result would be one where legitimate business would send their valuable e-mail to fewer recipients, while the worst kind of spammers would continue to fill millions of mailboxes with offensive e-mails with impunity. A DNE registry is *not* the answer to ending spam. It will only hurt small businesses. It should *not* be supported.

The final piece of solving the spam problem lies in consumer education. Unfortunately, and entirely innocently, many people have exacerbated their spam problem by leaving their e-mail address in chat rooms, on personal or business web sites, or various other places where spammers can grab them. Effective consumer education can go a long way to curb this problem and any initiatives in this area should be supported.

Spammers must be stopped while small businesses must be protected. It can be done only with an effective combination of national legislation, broad adoption of a universal technology that removes the anonymity of bulk e-mailers, and consumer education.

Testimony

Mr. Chairman and Members of the Committee, I want to thank you for your invitation to testify today regarding the effects of spam on small businesses. My name is John Rizzi and I am the President and CEO of e-Dialog. My small business of 51 people, located in Lexington, Massachusetts, and with small offices in Los Angeles and London, today is 100 percent dependant on e-mail being an effective marketing and communications channel. E-Dialog is an e-mail service provider. Our mission is to help large companies do e-mail right. As an example, we work with industry leading companies such as Reuters, Charles Schwab, Schering Plough Pharmaceuticals, John Deere, JC Penny, Harvard Business School Publishing, Doubleday, Cendant, and the NFL. We are extremely pleased that so much activity is happening at the legislative level to bring about an end to spam. In this testimony I will address how the right legislation can help small businesses, and also what elements of legislation must be avoided so as not to hurt small businesses.

For context, allow me to give you a little more depth on my business, e-Dialog. By no means do we just blast out e-mail. We are a new kind of marketing agency that has an extraordinary level of technology, all developed by our own engineers, that allows our clients to have the most highly targeted and relevant e-mail possible for their valued customers. We do every piece required in the process of communicating via e-mail: strategy development, creative design, complex campaign management, e-mail transmission, data collection and reporting, transaction processing, response handling, and in-depth analysis. Our technologies allow us to create a specifically unique e-mail to each recipient on our clients' lists – whether to a few hundred farmers each with different farm equipment or to millions of football fans with different team loyalties. We advocate to our clients that they should send less e-mail, not more, and that they need to make every e-mail count. Further, everything we do is based on permission. We do not send spam. Despite the fact that our e-mail is entirely driven by the consent of the recipient, increasingly our resources are focused on ensuring our clients' e-mail simply gets delivered.

I also want to point out that e-Dialog is a member of the NAI E-Mail Service Provider Coalition (“ESP Coalition”). This is a group of over 40 competitors in our industry, almost every one of them a small business, that are struggling with the onslaught of spam, as well as the emerging problem related to the deliverability of legitimate and wanted e-mail. The members believe that much can be done to solve the problem of spam. We have worked together to establish industry standards for sending legitimate e-mail, developed blueprints for universal technologies that separate spam from legitimate e-mail, and actively participated however possible in the legislative process so that effective laws are enacted. While I speak today on behalf of my company, e-Dialog, I also represent the combined interests of the ESP Coalition.

The small businesses that are members of the ESP Coalition are only a tiny fraction of the total number of small businesses using e-mail marketing as a business tool today. A report done by The Kelsey Group in September, 2002, estimates that 1.65 million small and medium enterprises (SME’s) are participating in e-mail marketing today, and predicts that the number will grow to 5.5 million in the next 4 years. This represents approximately 25 percent of all SMEs in the United States. The current users are already suffering badly from spam– the simple reality of cluttered mailboxes makes their messages hard to succeed. Additionally all the collateral effects of a spam filled world, such as message blocking or filtering either by internet service providers (ISPs) or desktop software, stops messages from going through without any notification that they didn’t succeed. Finally, the patchwork of 37 states with differing spam laws can paralyze the most determined legitimate e-mail marketer who is not interested in breaking the law.

I would wager that each member of this committee, or a member of your family, has unknowingly been negatively affected by the current tools meant to save you from spam. Many ISPs, acting as agents on behalf of their subscribers, filter the e-mail that comes through their systems to block spam. But they also catch a huge amount of legitimate e-mail as well – what we call “false positives.” A personal example for me is that my church can not get e-mail through to my wife – it is blocked by our ISP probably because

the church unwittingly uses a mail server located in a domain on the internet our ISP considers to be a source of spam. As such all mail from that domain is blocked, and messages from our church about choir practice for our seven year old daughter, or social action events my wife is interested in are lost. But we do not know they are lost, nor does the church, until after an event is missed. Small businesses suffer exactly the same problem, but their customers can be less forgiving than even my 7 year old. Recent research has suggested that false positives may be as high as 15% of all legitimate mail.

With all these challenges, why are so many small businesses even daring to engage in e-mail marketing? Simply, e-mail marketing is the most cost effective way for small businesses to communicate with their customers. E-mail is easier and far less expensive to produce and deliver than direct mail pieces. Businesses get immediate feedback and results – they can see if their audience is reading the mail and learn from what they are clicking on and adapt as necessary. They can easily drive customer loyalty and repeat sales which are the life blood of small business. Very importantly, e-mail allows a small business to extend its reach across city and state borders and begin to serve a national, if not international customer base quickly and cheaply. Overall, e-mail marketing done right allows small businesses to compete with larger companies by erasing the gap in the quality and reach of marketing communications a small company can afford vs. a large enterprise. As a small business operator myself I am predisposed to do business with other small businesses whenever possible. I notice that today I buy tea from SpecialTeas in Stratford, Connecticut; I buy toys for my daughter at Suzi's Dollhouses in Athol, Idaho; and car parts for my classic car at 3SX Performance in Charlotte, North Carolina. I would not do any business with these small shops if it wasn't for the valuable e-mail communications they provide. It's that simple, their businesses are better and wider reaching because of e-mail.

While the issue of spam gets all the attention, the fact is that consumers prefer to receive e-mail communications and promotions from the organizations and companies they know and do business with. According to a study conducted in July of this year by DoubleClick, one of the largest ESPs:

- Permission-based e-mail is the preferred method of contact from the favorite retailer regarding new products, services or promotions (preferred by 59% of consumers), while only 32.1% preferred direct mail, and 0% telephone.
- Permission-based e-mail motivates consumers to purchase: 67% of online shoppers have purchased as the result of clicking on an e-mail link.

It should also be noted that small businesses already take their e-mail communications very seriously. They agonize over the right content, the right offers, the right colors. While the sending of e-mail has been simplified for small businesses through readily available services on the internet, the actual process of conducting an e-mail campaign for a small business can be daunting. Very simply the small business owner cherishes his or her customer relationships and treats them appropriately. The last thing they need to worry about is 50 different state laws. One law, however, that is enforceable on a national level and predictable and manageable in its conditions can more easily be understood and complied with. In my business I have three full time professionals focused on deliverability issues, compliance with self-regulatory industry guidelines that we have committed to, and existing legislation. In other words 6 percent of my payroll is spent on this complex process. I'm lucky in that this investment supports the efforts of many clients, however the effort would hardly be less if my business was only serving itself. Individual small businesses can not afford the required level of effort to comply with more than one law.

Stopping spam is no easy matter. It will require a combination of fair national legislation, technology innovation, and a certain level of individual responsibility. Legislation alone will not stop spam, and in fact it's possible that no law will even put a dent in the worst kind of spam. The most important single fact to understand is that today's spammers are already breaking many laws. They are deceptive, greedy, unscrupulous people who don't hesitate to fill our mailboxes, and those of our youth, with obscene and offensive material, and for products and solutions no different than the snake oil peddlers of the past. The ubiquity and technology of today's internet allows these law breakers to hide behind false identities and vanishing store fronts. The public

outry about this type of spam is fully justifiable – it has to be stopped. But if you stop and ask anyone complaining about this sort of e-mail if there is any commercial based e-mail they like to receive they will surely say yes. And that's the conundrum. Let's look at each piece of the solution that will help, or potentially hurt, small businesses:

Legislation Against Spam

Small businesses do not want to break the law. The problem they face today is too many inconsistent and duplicative state laws. The investment any small business would have to make to keep up with these laws is prohibitive. Worse, they might be breaking a state law and not know it since the physical location of an e-mail recipient is often impossible to identify. Since e-mail is an inherently interstate medium preemption of state laws is critical so that small businesses will have a predictable and stable foundation from which to build their e-mail operations. Further, a national standard would allow enforcement officials to pursue spammers across state lines – something that is proving problematic today. I am pleased to see that the current bill approved by the Senate includes preemption and encourage the members of the House of Representatives to take action on spam legislation as quickly as possible. We need to secure the legislative environment as quickly as possible so that enforcement officials can pursue spammers aggressively and effectively.

A problematic aspect of legislation is the potential creation of a national do-not-e-mail (DNE) registry. A DNE list is full of challenges that a small business can not afford to uphold. For a DNE to work very clear and strict definitions would have to be created, and complex technology would have to be adopted. Meanwhile, e-mail is a continually evolving medium so definitions and technology are unlikely to keep up with changes – and loopholes will be found. This will drive lawsuits, and small businesses will suffer. This is worth thorough explanation. Here are some of the open questions and challenges a small business would face with a DNE list:

- Many small businesses have already built a significant and valuable asset in their permission-based lists over time. Will the new DNE list apply to these existing lists or only to new names that come onto the list? Will businesses need to reconfirm all their permissions to ensure compliance? If so, this could cause a list reduction of between 50 and 80 percent, leaving the business to essentially start over in building their lists.
- Security concerns are daunting. The DNE list will need to be accessed millions of times per day by every e-mailer in America. The balance of providing easy access and high security is nearly impossible. The first hack into the DNE list (unfortunately unless someone invests in NSA/CIA level security on this database, there *will* be a hack) will be disastrous. Unscrupulous spammers will have their hands on the list and will be mailing to it within hours. The resulting tidal wave of spam will be unstoppable.
- Potential consumer confusion and annoyance. Customers who value the e-mails they receive from legitimate e-mailers may join the DNE list to avoid the other e-mails they do not want. They will get annoyed at their favorite stores because they are now uninformed or did not receive a special announcement. To avoid this, there would have to be a way to selectively override / get off the DNE list for specific mailers, but not for others. This would add dimensions of complexity no small business could support. Ironically, the DNE list would stop the good marketers from reaching your mailbox but would do nothing to stop the worst kind of spam from existing lawbreakers. The consumer will end up extremely frustrated when he or she realizes that signing up for the DNE list completely backfired.
- Small business implementation and maintenance costs will be prohibitive. Just getting educated and equipped to comply will be expensive. Then the added effort of regular compliance will add continuing expense to doing e-mail, erasing one of the greatest benefits of the medium. Further, the business operator will

start taking calls from disgruntled customers who missed an important e-mail announcement and will spend valuable resources sorting out what happened and “making good” for their valuable customers.

- Many e-mails from legitimate companies can be both informational and promotional. Newsletters and event announcements are frequently supported with sponsor ads. (A shoe store newsletter may include an ad from Nike for example). Transactional e-mails also include valuable promotions for additional products and services. Not unlike free subscription trade magazines which contain ads, trade level e-mails might include ads. Who’s to judge whether these e-mails are spam? For example, is the announcement of a new fashion trend or new generation of products and services informational or promotional? What is the sender to do?
- Finally, a DNE list may do nothing to eliminate or reduce the worst offenders. Worst offenders will not honor the DNE list. Huge percentages of spam messages have content that is already illegal.
- While many of these questions can be answered with common sense, the fact is that wherever there is a question there is an opportunity for a law suit, and small businesses are likely targets for “spambulance-chaser” lawyers to find a quick settlement.

Technology to Stop Spam

We must first remember that the problem we have in our mailboxes is not e-mail sent from small businesses. It is bulk mail sent indiscriminately by bad actors to any e-mail address they can find no matter how irrelevant their message is to the recipient. The architecture of the internet allows spammers to hide, they spoof identity, and they deceive recipients with misleading “from” and “subject” lines. This sort of deceptive bulk e-mail can be stopped with the development and

adoption of a universal authentication and grading system for large mailers. The ESP Coalition has been working on “Project Lumos” which addresses this exact solution and is drawing broad support from both large commercial and corporate e-mailers. Essentially, Project Lumos is designed to force senders of volume e-mail to incorporate authenticated identification into every message sent. The use of authenticated identity, along with a rating of sending practices over time, prevents spammers from hiding behind the technology of e-mail and forces all senders to be accountable for their sending practices. I will submit a more thorough description of this effort along with my testimony.

Adoption of this sort of technology will make all mailers identifiable, and therefore accountable, for what they send. Legitimate small businesses will be supportive of this since their e-mail is well received by their audiences. Further, the effort and cost to comply with this technology for SMEs will be minimal.

While this is mostly a private industry effort right now the FTC has expressed support. I like to believe this can remain in the private sector, like many standards on the internet, and I am very encouraged by the current cooperation and support by many parties.

Individual Responsibility against Spam

I don't receive much spam at my personal e-mail address that I've had for eight years, and I know why. Conversely I receive a ton of spam at my business e-mail address, and again I know why. I have been in e-mail technology and/or service related businesses since 1989 so I have a long understanding of how it all works. I've always been extremely careful with my personal e-mail address and it has paid off— spammers haven't found it. Unfortunately my business e-mail address is very public; it appears on our web site and on press releases. Spammers harvest this address easily and add it to their lists. My e-mail box is an ugly place. This

all speaks to the fact that consumers need to be educated so as to know what they should and shouldn't do with their e-mail addresses. It is unfortunate but true that there are countless ways a person can unknowingly sign themselves up for a spam list. A little education can go a long way to stop this. Unfortunately, I don't know of any public effort to educate consumers on the perils of e-mail and spam. I expect that with a little nudging, however, various consumer groups would be happy to help with this cause.

Conclusion and Recommendation

We are all frustrated by spam and want it eradicated from our lives. Several years of debate have now brought our federal lawmakers to the very cusp of taking definitive action to end spam. It must be acknowledged, however, that the best possible law still does not solve the problem alone. The law must be combined with new technology and consumer education. The technology must achieve the primary goal of removing anonymity from spammers so that they can not hide from the law. The technology must also be universally available at a very low cost to any size business so that legitimate and respected marketers, as well as consumers, do not lose the great benefits that e-mail can provide. The law must also be preemptive of any state laws so as to simplify compliance and enforcement.

The most important immediate step is to act quickly and definitively to approve the CAN-SPAM act approved by the Senate last week. The only recommend revision from the Senate version is to move the effective date up to January 1, 2004. It is crucially important to small businesses that the law does not require the creation of a Do-Not-E-mail registry.

The next step is to support industry initiatives in the development of a standard technology that when deployed will force authentication of large mailers so that

spammers can not hide. The final step is to support consumer and industry groups in providing better education to consumers so they don't unwittingly fall prey to spammers.

Mr. Chairman, thank you again for inviting me to testify on this very complex problem. I am excited that a workable solution is within our grasp that can both stop spammers and protect small businesses.

I look forward to any questions you may have.



TESTIMONY OF CATHERINE GIORDANO

ON BEHALF OF WOMEN IMPACTING PUBLIC POLICY

BEFORE THE SUBCOMMITTEE ON REGULATORY REFORM AND OVERSIGHT

OF THE

HOUSE COMMITTEE ON SMALL BUSINESS

“SPAM AND ITS EFFECT ON SMALL BUSINESS”

OCTOBER 30, 2003

Good morning Mr. Chairman and Members of the Subcommittee, my name is Catherine Giordano and I am President of Knowledge Information Solutions, Inc. (KIS), located in Virginia Beach, Virginia. I am appearing today on behalf of Women Impacting Public Policy (WIPP), a national bi-partisan public policy organization, advocating in behalf of women in business, representing 460,000 members. I serve as a Co-Chair of WIPP's Procurement Committee.

KIS is a woman owned, 8(a) Certified small business, which employs 47 workers. We provide computer products and IT services such as ISP Internet and wireless connectivity and network design and consulting. We supply IT products and services to the federal government through 11 government-wide acquisition vehicles to approximately 47,000 customers.

I would like to thank you, Mr. Chairman, for inviting me to speak on a subject that my company deals with on a daily basis and one that I believe is very costly to small businesses – spam. Coincidentally, KIS just recently completed an internal analysis of the effect of spam on our business and so this testimony is very timely to our company.

Most business environments are now computer based. At KIS, our small business is reliant on a communication system to our customers that is by electronic mail and correspondence predominately through computer technology. Any consideration to shut down the flow, block or filter all incoming traffic would be to the detriment of our e-business environment and to business in general.

In addition, small businesses are always interested in attracting new customers and we are ever mindful and concerned about annoying current or prospective customers. Therefore, KIS offers a form of permission-based customer marketing that will readily

remove their name from any KIS mailing list upon request. This practice is typical of most other small businesses. Legitimate businesses take these requests seriously and honor requests to remove names from the list.

Unsolicited commercial electronic mail, spam, represents 30% of KIS inbounds correspondence. It is an ongoing process and becomes more expensive as the innovation of “global” spam capabilities has shifted the burden of cost from the sender of the spam to the small businesses, ISP providers, and the customer. Since spammers continuously change their methods of operations, we spend additional employee time to find just the right mix of settings and adjust them.

Our review shows that KIS’ small business customers spend an average of 7 minutes per day per person dealing with spam. Since KIS provides 250 small businesses in the Southeastern Virginia Region information technology management and ISP support services, we estimate that the total cost in lost productivity for these customers is estimated to be \$2.9 million. Mr. Chairman, \$2.9 million could be used much more productively by small businesses on items such as equipment purchases, creation of jobs or providing health care to employees.

I will just take a minute of the Committee’s time to explain how spam filtering works on enterprise systems. Most enterprise spam filters implement more than one filtering method, thus giving the user a choice to delete suspected spam before it reaches the user’s inbox, quarantine suspicious messages, or tag suspicious messages so that the end user can choose what to do with unsolicited messages.

Enterprise spam filters offer a wide range of abilities, features and costs. The filters fall into five general categories: (1) Client-Side Filters - software installed on the

client workstation that will attach to their mail software and assist with the filtering and identification of spam; (2) Groupware Plug-ins- software that directly connects to the groupware application to filter mail as it is transmitted internally; (3) Internal Simple Mail Transport Protocol (SMTP) Proxies - servers placed at the perimeter of the organization to capture spam before it is transmitted to the internal network for distribution; (4) appliances - internal SMTP Proxies installed on the network perimeter to capture and filter spam and (5) Hosted SMTP Proxies - third-party companies where all mail is collected and filtered and then transmitted to the end users' network for distribution.

KIS currently utilizes DNS - Domain Naming Service - the protocol for translating names into IP Addresses. For example, an address like - www.google.com - must be converted into 216.239.41.99. One of the options to filter spam through DSN, called blacklisting, typically catches only 25% of these emails. Filters utilizing keyword searching will catch an additional 5% of the emails. The number of false positives (email wrongfully identified as spam) raises daily as more and more companies are inadvertently submitted to the BlackList servers. Of the emails caught by DNS blacklisting and keyword searching, 2-5% are false positives. The cost associated with identifying false positives is roughly \$2,499 annually. Estimated yearly losses of employee productivity after KIS current anti-spam measures are an estimated \$93,750.

To implement a KIS internal full-blown perimeter/mail-server incorporated spam detection system costs our customers \$4,500 plus the cost of equipment hardware. Their return on investment after implementation of full-blown spam detection software is estimated at 5.5 months.

As the Committee knows, the Senate in the last several weeks passed an anti-spam measure by 97-0. Although WIPP has not had the chance to review the proposals pending before the House in depth, our thoughts are twofold. One, spam is a costly expense for small businesses. Two, when enacting legislation to limit spam, Congress should take into account the effect of its actions on small business compliance.

When considering a new law to prevent spam, our members do not want the burden of seeking permission from every customer in order to send an email. The FCC's proposed regulation on the "Do Not Fax" rule recently is a good example of good intentions by the government agency but bad consequences for small business. The proposed rule would require every business to seek permission from every customer before faxing things like invoices and other necessary business communications. WIPP heard from many of its small businesses that such a requirement is simply not practical when trying to restrict unsolicited faxes. Similarly, such a system for email communications would be onerous for small businesses. Compliance with an "opt-in" is problematic for small businesses with limited resources.

In closing, I would like to quote from the testimony of Ms. Paula Selis, Senior Counsel, Washington State Attorney General, delivered before The Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection Subcommittee on Telecommunications and the Internet on July 9, 2003...

- "Strong legislation is only one part of the solution. As a state attorney general's office, we believe that consumer education is also important, as is the advent of technology. If legislation is passed, it must be flexible

enough to allow for new technologies that may ultimately be more effective than any law. There is no easy fix to this problem, and it will take all the tools we have to address it. In conclusion, we support the work of this committee in tackling the enormous and growing issue of spam. We urge you to pass a bill that is as strong as possible-that gives consumers and ISP's adequate substantive protections, and creates sufficient deterrence and meaningful enforcement mechanisms to take the profit out of spam."

Ms. Selis' statement summarizes WIPP's approach on spam. There is no question in our minds that limiting spam is good for small business. The solution, however, must take into consideration the compliance costs to small business.

I would be pleased to answer any questions.

Prepared Testimony of
Shane Ham
Senior Policy Analyst, Technology and New Economy Project
Progressive Policy Institute

House Committee on Small Business
Subcommittee on Regulatory Reform and Oversight
Hearing on "Email Spam"
October 30, 2003

Chairman Schrock, Representative Gonzalez, and Members of the Subcommittee:

Thank you for inviting me here this morning to discuss the grave and growing threat that unsolicited commercial email, or spam, presents to the future of e-commerce and the Internet. The Progressive Policy Institute has been sounding the alarm on the spam problem for years, having released our first report on the topic in 1999. Over the past four years, Congress has tried several times to reach agreement on spam legislation, with no success, while in the meantime, the problem has worsened significantly. This led PPI to recently release another report on spam calling for even tougher legislation to deal with the problem.¹

Make no mistake about it, spam is getting worse every day, at an almost exponential rate. Hard numbers on spam are hard to come by, but every major study of the problem agrees that spam reached an important tipping point within the past year: there is now more spam crossing the Internet every day than there is legitimate email. More importantly, the explosion of spam is starting to destroy the usefulness of email. According to a recent survey by the Pew Internet and American Life Project, more than half of all email users say that spam has made them less trusting of email in general, and one in four users have curtailed their use of email in an effort to avoid spam. If we have learned anything over the past few years, it is that those numbers will only get worse.

In PPI's view, there is no question that legislative action to stem the flow of spam is long overdue. The details of a legislative solution are still the subject of considerable debate, as demonstrated by the fact that there are three major bills in the Congress offering different solutions: H.R. 2515 (the "Anti-Spam Act"), H.R. 2214 (the "Rid Spam Act"), and S. 877 (the "Can Spam" Act). Though these bills vary in the details (and none goes far enough, in our opinion), they all have the substantially similar effect of bringing a regulatory framework to unsolicited commercial email rather than an outright ban, as Congress did with junk faxes in 1991.

The pertinent question before the subcommittee today is what impact, if any, a regulatory framework will have on small businesses. **I believe that small businesses are hurt by unsolicited commercial email far more than they gain from using it as a marketing tool, and therefore on balance, small businesses will benefit from the strongest possible anti-spam regime.**

Is Spam Useful to Small Businesses?

While there is little doubt that unsolicited commercial email can be useful to individual firms -- especially those who use spam as their primary or sole marketing method -- the overall impact of spam on small business is neutral at best. There is no evidence to suggest that any marketing technique (much less a marketing technique as reviled as spam) has a positive impact on overall consumer spending, which generally only varies in response to larger variables such as discretionary income levels, consumer confidence, and so on. **Marketing, including spam, can change the mix of consumer spending, but not the overall amount of it.** Therefore, the argument that eliminating spam will cost jobs is not compelling.

Moreover, as the spam problem gets worse -- with more and more fraud artists using spam to find victims -- the use of email for marketing will begin to favor those firms and products with high name recognition. To the extent that the average email user responds to spam -- and the response rates are extremely low -- they will be much more likely to respond to an email solicitation from a trusted company with a well-known reputation than from an unknown small business. **Fairly or not, small companies seeking to expand their customer base will be lumped together with scammers and pornographers and have their solicitations sent straight to the trash.**

Is Spam Harmful to Small Business?

Most small businesses, just like most large businesses, use email as a tool to conduct transactions and communicate with existing customers far more than they use it for unsolicited marketing. Therefore, the vast majority of small businesses have a strong interest in preserving the effectiveness of email in general, even if it means reducing the effectiveness of spam.

The implications for the entire email system aside, spam imposes higher costs on **small businesses than on the average user.** There are several reasons for this:

- In general, small businesses send and receive far more email than individual users and rely on email much more as a critical business tool than individuals, who may use it only for sending notes to friends. A degeneration in the effectiveness of email as a communications tool, therefore, will hit small businesses disproportionately hard.
- Small businesses must be easy to contact, so they do not have the option of using a false "spam bait" address, or frequently changing addresses, or "munging" addresses (i.e., shaneham@REMOVETHISexample.com) to make them invulnerable to software that harvests email addresses from the World Wide Web. These are standard tricks used by many email users to keep the amount of spam to a manageable level, but are unavailable to small businesses. The more that individual users take advantage of these tricks, the more the burden of spam will

fall on small businesses, as they will be the easiest source of valid, regularly checked email addresses for use by spammers.

- Small businesses use filtering software at their peril, since no software can guarantee that only spam will be discarded. Since most filters utilize a “white list” so users can guarantee that email from known senders gets through, individuals may be willing to accept the tradeoff of losing the occasional email from a high school chum in exchange for getting rid of the hundreds of spam messages that would otherwise flood the inbox. Small businesses, on the other hand, live and die by communications from strangers -- also known as “prospective customers.” The tradeoff of losing legitimate email is not worth it for many small businesses.
- Small businesses, with limited staff and resources, are least able to devote time and energy to wading through the flood of spam in order to find the mission critical email. If the volume of spam continues to increase at the current rate, it will soon become far too much for average small businesses to deal with, forcing them to resort to one of the less-than-ideal options above.

One other factor working against small businesses is the fact that they are least equipped to deal with the patchwork of state laws that currently govern spam. Because it is nearly impossible to be certain of the physical location of an email recipient, email is the communication medium least able to be governed on a state-by-state basis -- even broadcasting provides more certainty than email. **Small businesses, therefore, need federal preemption of state spam laws even more than large businesses**, which at least have legal and IT departments capable of managing the risk of sending a spam that violates the law.

For all of these reasons, it is our view that while spam may offer an individual small business marketing advantages, for small businesses as whole, spam imposes more costs than benefits. Therefore, we believe that small businesses need Congress to impose some sort of control over the spam problem even more than the average individual needs it. Again, if Congress delays too long, the public demand for an outright ban on unsolicited commercial email will become overwhelming, and small businesses will have no chance to benefit from unsolicited commercial email even if they want to do so.

Can Legislation Stop Spam?

One claim frequently put forth by opponents of anti-spam legislation is that only the legitimate email marketers will be deterred, while unscrupulous pornographers, con artists, drug dealers, and overseas spammers will continue to flood inboxes. While it is certainly true that no legal prohibitions will stop all spam (any more than speeding laws stop all speeding), Congress should nevertheless act in order to stem the problem and keep it from getting worse. The most important reason is that the federal government has no rules with which to go after the “gray area” spammers who do not follow accepted best practices for unsolicited commercial email but who are not selling illegal or

fraudulent goods or services. But we must also keep in mind that even "legitimate" unsolicited commercial email is still a problem -- spam is spam.

Another argument against effective anti-spam legislation is that "legitimate" advertisers will see their ads go into the trash while only the criminals get through. **The fact is that millions of email users want to stop all spam, and don't distinguish between legitimate and illegitimate spam.** The same argument was applied to the "Do Not Call list" debate, and Congress rightly decided that the preference of Americans not to be bothered in their homes outweighed the damage that would be done to telemarketers. Because there is more at stake with spam, the same logic applies even more strongly in this case.

What Provisions Should Anti-Spam Legislation Contain to be Effective?

The three major spam bills represent literally years of negotiations on important matters such as a private right of action, the role of state enforcement, the level of criminal penalties for fraudulent routing information, and so on. However, an effective anti-spam law would have two important provisions not currently contained in any of the major bills:

Require a standard identifying label such as "ADV" in the subject line of all unsolicited commercial email. This is perhaps the most important weapon in the fight against spam. By requiring a standard label -- not just a notice that the message is spam, but a single standard identifier -- both email users and ISPs can easily configure software to reject spam. Because spam, like junk faxes, shifts costs onto the recipient, it is only appropriate that spammers be required to make filtering as simple and inexpensive as possible.

All three bills require a standard identifier (e.g., "ADULT") for sexually explicit spam, but balk at requiring a standard identifier for all unsolicited commercial email. While all three require the Federal Trade Commission to study the effectiveness of such a solution, I am concerned that Congress might not be able to implement such a standard in new legislation even if the FTC recommended doing so, given the difficulties in passing anti-spam legislation over the past several years -- the opposition by the spam industry will be too great, while the political support for a second anti-spam bill may not be strong enough. Moreover, experts agree that the standard label would be extremely effective; indeed, the effectiveness of such a solution is exactly why it is so fiercely opposed by the spam industry.

Create a "universal opt-out" by authorizing and appropriating funds for the Federal Trade Commission to create a Do Not Spam list. In our 1999 report, PPI called for further study of the idea of a "wash list" -- a list of email addresses that cannot be legally spammed -- because we felt that such a drastic step was premature. Since then, two things have happened to make a Do Not Spam list necessary. First, unscrupulous spammers have included supposed opt-out statements in their spam that serve only to verify the validity of an email address. Many email users now understand that clicking on an opt-

out link in a spam message is a surefire way to get more spam, and rightly refuse to do so. Second, the FTC is moving ahead with a Do Not Call list to limit telemarketing calls into the home. Because mandatory opt-out procedures are no longer effective, and because the FTC will have experience in creating a wash list, now is the time to build the Do Not Spam list. This will enable email users to opt out of all spam, and would likely prove to be just as popular as the Do Not Call list. Of course, the list would not be made available to the public, but rather spammers would be required to "wash" their recipient lists against the FTC list to remove any addresses that have requested not to receive unsolicited email. Failure to comply with the wash list requirement should result in criminal penalties, at a minimum, on par with the false header penalties.

The Senate bill asks the FTC to study the technical problems associated with creating a Do Not Spam list, and indeed implementing such a list will be more difficult than its anti-telemarketing counterpart. In order to keep the addresses secure, it might even require that the FTC set up servers to act as "remailers" to forward commercial email to recipients after washing out the registered addresses. Because of the technical difficulties, the authorization to implement the list contained in the Senate bill needs to be backed up with appropriations if the FTC is to have any hope of moving forward with this important solution.

Conclusion

Because small businesses stand to gain from effective anti-spam legislation even more than individual users, it is imperative that Congress act quickly. But there is a tremendous risk that an ineffective spam law will fail to stem the flow of spam, decreasing the usefulness of email itself. It would be unfortunate if the most successful Internet application was slowly strangled to death by the weight of spam. Congress has the opportunity to ensure that doesn't happen, and should use this chance to pass an effective law that will save email by drastically curtailing spam.

¹ Our reports on the spam problem can be found at our web site, <http://www.ppionline.com>

Testimony of

Clyde Wayne Crews Jr.
Director of Technology Policy
Cato Institute

**Before the Subcommittee on Regulatory Reform and Oversight of the Committee on Small
Business of the United States House of Representatives**

“Spam and its Effects on Small Business”

2360 Rayburn House Office Building

October 30, 2003

The increasingly apparent downside of an Internet on which you can contact whomever you want, is that anyone can contact you.

Unsolicited commercial email, or “spam,” is unquestionably a huge problem. Bulk spammers pay no postage. Ultimately, the resolution is to shift costs back to the sender. The question is whether that should happen legislatively, or via technology, pricing, industry consortia, or some combination.

Ironically, a recent Reuters story indicated that filtering in some ways is becoming too powerful, as even friends are required to jump hurdles to get into their acquaintances’ white-listed, moat-surrounded mailboxes. It seems the “openness” that was central to the “Internet experience,” as the marketers like to say, is now a bug. It seems no longer the case that everybody necessarily needs or wants to be connected to everybody else, or shares conforming views of what acceptable online etiquette entails.

However, the real issue isn’t merely that legislation likely won’t rid us of spam (given the Net’s global pool of scofflaws); rather, legislation like “ADV” mandates or “do-not-spam” lists don’t address the fundamental factors at the root of the spam problem: (1) lack of authentication of senders, and (2) the ability of spammers to shift the costs of sending bulk email to recipients.

As for those legal attacks on spam being debated, some are appropriate and necessary. Such misdeeds as peddling fraudulent merchandise, or forging the name of a person or organization as the sender of a spam should be punished, as should phony “unsubscribe” promises, as should breaking an agreement made with an Internet service provider that prohibits bulk mailing. The law also should go after those that invade computers, such as by launching programs that hijack and send out spam from third party computers. Abusive forms of spam like “dictionary attacks” and spoofing seem related to hacking more than to commerce. Such behavior is already illegal of course.

To a great extent, unfortunately, legislative commands will be ignored by the most egregious spammers, and alternative solutions are going to become more urgent.

Maybe that's a blessing in disguise, because even spam itself is not a single dilemma and may require different responses anyway: for example, solving the problem of kids seeing porn in the inbox is a different than solving the problem of ISPs overwhelmed with Viagra ads.

Market solutions, unlike legislative decrees, better lend themselves to cross-problem application, beyond spam. For example, just as the emerging email problem was anticipated years ago, one might similarly predict problems emerging as costs imposed on Internet service providers by free file-sharing services like Kazaa escalate. Spam (getting stuff) and piracy (taking stuff) alike are partly fostered by a pair of broader features: the lack of tiered pricing for network use, and the ability to hide one's identity or origin online. The Internet's "all you can eat" buffet may need to end for email and file-sharing alike, a different proposition from passing a law.

The Internet wasn't originally designed to be the mass commercial and consumer medium that it is today. If one were to design a commercial network today from the bottom up, it would probably incorporate authentication of the senders of email. Indeed, changing Internet plumbing in midstream to allow verification of sender origin wouldn't aid just the spam problem but also cybersecurity and hacking concerns that industry needs to address perhaps more urgently even than spam.

Legislation shouldn't stand in for or delay the day of reckoning for what should be (perhaps must be) a technical or organizational or market-driven fix. But one thing is clear: If the industry doesn't solve spam, the law will step in, in ways some legislative proponents may come to regret.

Proposed legislation, for example, would impose subject-line labeling requirements for commercial email (commercial messages would have to say "ADV"); mandate an "unsubscribe" mechanism; ban the use of "harvesting" software; set up stiff non-compliance fines or even bounties; and establish an expensive (and likely hackable) Do-Not-Spam list at the Federal Trade Commission.

But if legislation sends the worst spammers offshore, all we'll have accomplished is legal and regulatory hassles for small businesses trying to make a go of legitimate e-commerce, and mainstream companies that already follow "best practices" like honoring "unsubscribe" requests.

Besides, commercial e-mail, even if unsolicited, may be welcome if the sender is selling legitimate wares in a non-abusive manner. Most of us can agree on the outrageousness of the porn that hits our family in-boxes. But, on the other hand, thousands of people bought "The World's Smallest Radio-Controlled Car" at Christmastime, or the Most-Wanted card deck during the Iraqi war. .

Proposed legislative penalties can easily keep many small businesses out of Internet marketing altogether, for fear of a misstep. Is that really our goal? (It takes effort to unsubscribe addressees, and inadvertent mistakes will happen.)

We should guard against unintended consequences, especially given the difficulty of enforcing legislation against the actual culprits. How might the definition of “spam” expand? Is it just “bulk unsolicited commercial” mail, or is it “anything you didn’t ask for?” Many say the latter.

What will be the consequences of legislation for noncommercial e-mailers like nonprofit groups that send in bulk? Many things aren’t commercial but are still unwanted: press releases, resume blasts, and charitable solicitations. I’ve even seen the term “scholarly spam” for material like that sent by organizations like my own.

Notably, politicians exempt themselves from anti-spam legislation, remaining free to send campaign material. But if we need “ADV” for commercial advertisements, then what about “REL” for religious “spam” like a piece I received warning of the coming apocalypse?

We shouldn’t discount the creativity of lawyers looking to sue easy marks, given that the bad guys will often be out of reach. Rest assured lawyers will go after those who occasionally slip up when implementing “unsubscribe” requests, or after newsletters that contain embedded ads but that might have failed to put “ADV” in the subject line. Navigating the treacherous email commerce of tomorrow will be easier to handle for large firms relative to small firms. Is this fair?

The invective around spam is so heated that you don’t know whose line you’re going to cross. Some of us occasionally send an unrequested email to strangers with a link to our company affiliation in our email signature line. That’s a subtle solicitation, whether we admit it or not. Remember, “spam” is a made-up word, subject to interpretation.

Aggressive pop-up ads may become targets in the aftermath of spam legislation, too (they already are in Germany). They’re not e-mail, but they are unsolicited and commercial, and getting more insistent than ever, employing animation and sound. Some ads aren’t merely pop-up but take over the screen.

As for 1st Amendment concerns, legal bans on “pseudonymous” e-mail return addresses can affect untrammelled speech and anonymity for individuals, and will be ignored by spammers anyway. Well-meaning individuals can use “spamware” to create the contemporary version of the anonymous pamphlets that have played such an important role in our history.

That said, while I don’t want the government to outlaw anonymous emailing, the private sector may need to prohibit it on private networks if that’s what canning spam requires.

Another worrisome issue is the tendency of legislation to set up “rules” for advertising. Indeed, much of the Internet industry’s newfound support of email “spam” legislation seems

defensive and aimed at protecting the right and ability to send legitimate commercial email. Those motives are understandable and appropriate.

But there can be a downside to seeing legislation as the avenue to legitimacy. Surely, post-legislation, marketers will feel that they have met federal requirements, like ADV and a street address, and therefore ISPs have no right to block their messages even if the ISP would prefer not to deal with them. (One commenter said the "CAN SPAM" bill meant that you "can spam.") In that environment, would advertisers be able to sue whenever their mail gets filtered or blacklisted, even in the absence of a contract with the ISP? Blacklists are one of the key means of dealing with spam today. I want to permit and retain ruthless blocking by ISPs, not have that ability over-ridden by the fact that a business followed some legislative checklist. Contracts, not legislation, must rule here. ISPs must retain the right to end such unwanted relationships.

Either the industry or Congress can set terms, but hardly both.

There's some good news. If the desire is to stop spam in personal inboxes, one can do it already, without legislation. So-called "handshake" or "challenge-and-response" email accounts do not allow any email through from strangers unless they respond to a "challenge," such as supplying a generated password or answering a query. In over two years, I've never received a spam in one such account that I use: That doesn't mean I won't. But because the most offensive spam is sent by automatic bulk mailing programs that aren't capable of receiving a reply, spam no longer appears in the inbox. Whatever legislators do, however, white-lists or such challenge-style systems are essential for children's accounts.

There are significant transitional costs to changing the default expectation from today's "everything comes in unless you say 'no'" to "nothing comes in unless you say 'yes,'" but the spam problem is so bad that there may well emerge a culture of tolerance, an expectation that e-mail recipients from now on will ask you, "Who's there?" at least the first time you come knocking.

Meanwhile, service providers need to get busy on standards, such as for authentication of senders. Identifiers or "seals" for trusted commercial e-mail could be a critical means of helping tomorrow's ISPs block unwanted e-mail, but it could require major reworking of Internet protocols, and unprecedented industry coordination. A new consortium including America Online, Microsoft, and Yahoo to establish Trusted Sender standards like those long called for by TRUSTe would bolster this approach.

Such major overhaul of the Net architecture has been likened to widening all the nation's roads six inches. It is a monumental undertaking. But if it truly is the case that lack of authentication and pricing is at the root of the spam problem, legislation doesn't directly solve those issues. It may be that a system in which originators of messages remain anonymous is altogether inappropriate for a commercial information society of tomorrow. Maybe it needs to be impossible, not merely illegal, to send a commercial email if the network owner can't discern who you are via some form of origin certification or digital signature. If so, that's a job for the industry that can't be replicated by passing a law.

Already Commissioner Orson Swindle of the Federal Trade Commission has indicated he thinks the industry can do far more to address the problem on its own, such as by granting users more control over their inboxes. ISPs might also limit the number of outgoing messages per subscriber account, for example. MSN Hotmail recently did so, and Yahoo did it long ago. Yahoo also recently implemented a sort of reverse challenge-response. Users who suddenly started sending in bulk found themselves challenged by Yahoo.

Today's flat fees for sending email aren't a fact of nature or a natural right. Ultimately, email "postage" or protocols that allow users or ISPs to charge fractions of a cent for receiving unsolicited email would end bulk spam once and for all. Bonded sender programs are already being set up that might anticipate such a sea-change. But such innovations would be a long way off.

Given the understandable desire to stop outrageous unsolicited email, it is all too easy for Congress to undermine legitimate commerce, communications, and free speech, and delay needed changes in industry structure, relationships, practices and technologies. Meanwhile spam could continue pouring in from overseas. We need locked inboxes, authentication, and perhaps "postage" to allow users to customize their inboxes to reflect their own conceptions of "spam." Those solutions are even better if they are harmonious with other priorities like cybersecurity. The industry needs to get busy before Washington does.

Whether or not Washington passes an anti-spam law this session, the industry must still grapple with what are fundamentally technological and economic dilemmas rather than legislative ones. If industry doesn't resolve sender authenticating issues and end cost shifting, Congress will act—but without solving either problem.

###

