OFFICIAL TRANSCRIPT PROCEEDING

FEDERAL TRADE COMMISSION

MATTER NO. **P024407**

TITLE **SPAM PROJECT**

PLACE **FEDERAL TRADE COMMISSION**
600 PENNSYLVANIA AVENUE, N.W.
WASHINGTON, D.C. 20580

DATE **APRIL 30, 2003**

PAGES **1 THROUGH 309**

FTC SPAM FORUM -- DAY ONE

SECOND VERSION

FOR THE RECORD, INC.
603 POST OFFICE ROAD, SUITE 309
WALDORF, MARYLAND 20602
(301)870-8025

FEDERAL TRADE COMMISSION

I N D E X

For The Record, Inc.
Waldorf, Maryland
(301)870-8025

P R O C E E D I N G S

- - - - -

For The Record, Inc.
Waldorf, Maryland
(301)870-8025

MS. HARRINGTON: Good morning. I'm Eileen Harrington, and I'm very happy to welcome all of you to this Spam forum. Before I turn this over to the Chairman, we have some housekeeping announcements.

First of all, how many have one of these? Turn them off right now. We have a special honing device in this room that will capture your wireless address and Spam it incessantly --

(Group laughter.)

MS. HARRINGTON: -- if you don't turn it off right now -- right now -- right now -- right now -- right now -- turn it off.

Secondly, we've got some refreshments in the hall for breaks, and they were very generously provided by AOL, AT&T Wireless, Brightmail, Earthlink, EPrivacy Group, SpamCon Foundation, Word to the Wise and YAHOO, and we appreciate that a lot.

Third, this is a government building, more or less, and we have some information that we need to provide you at the request of our security people. In the very, very, very unlikely event that we have to have an evacuation, there are two exits, and both of them can be reached from the hallway that you entered through. One exit is straight back; the other is to the right and out the front door, as you came in. That's how to leave

if we have an evacuation.

Of course, our most special thing is sheltering in place, which we practice. And in the really unlikely event that we have to do that, go to the hall, so there's coffee and refreshments.

(Group laughter.)

MS. HARRINGTON: It will all be fine. Now, it is my great pleasure to introduce my boss, Tim Muris, who is the Chairman of the Federal Trade Commission. The Chairman, a couple of years ago, when he took the helm, worked with his colleagues to develop a very clear privacy agenda, and key on that agenda is looking at Spam, taking action against deceptive Spam and working to make sure we understand fully the nature of the problem.

So, today's forum, in a very real sense, comes as the result of that effort, of efforts that the other members of the Commission have made and I am just very pleased to introduce Chairman Muris, who will kick things off.

Mr. Chairman.

(Applause.)

CHAIRMAN MURIS: Good morning. We have some special guests here whom I'll introduce at the end of my remarks.

Welcome to our forum on Spam E-mail and thank

you very much for joining us. I'd especially like to thank our distinguished panelists for coming from all over the world to share their insights and expertise.

We convened this forum to explore the issue of unsolicited commercial e-mail, or Spam. Since I became Chairman, protecting consumers' privacy has become a principal focus of the FTC. Consumers are concerned about their privacy, including unwarranted intrusions into their daily lives. Spam is one of the biggest such intrusions.

Everyone enjoys reading e-mail they want, whether messages from friends or news about a sale at your favorite store. Today, though, our inboxes are clogged with unwanted, objectionable and fraudulent messages. Spam is threatening to destroy the benefits of e-mail.

What makes Spam different from other forms of marketing and why do we receive so much of it? One reason is that unlike telemarketing or direct mail, with e-mail it's easier to hide one's identity and to cross international borders.

E-mail can be sent from anywhere to anyone in the world, often without the recipient knowing who sent it. The class structure of e-mail is another difference between Spam and other forms of marketing. There are low

to no costs to send additional Spam. Instead, recipients and internet service providers bear most of the costs.

Because of these facts, as we know from our personal inboxes, the volume of Spam has increased dramatically. Even the FTC's inboxes have experienced this increase. Since 1998, the FTC has maintained a mailbox for consumers to forward their Spam. The messages are saved in a box-like computer storage device that we have dubbed the refrigerator, because it looks like a refrigerator.

During 2001, we received an average of 10,000 messages per day. Last year, that figure climbed to over 47,000. Currently we receive, into the refrigerator, over 130,000 messages each day.

In February 2002, I announced the FTC's first systematic crackdown on deceptive Spam. Since then, we have tackled Spam on three fronts: Law enforcement, education and research. To date, the FTC has announced 48 law enforcement actions targeting deceptive Spam. Soon, we will announce a settlement in the first FTC law enforcement action against false e-mail remove representations and e-mail spoofing, by which Spammers hide their identity through forging the from or reply lines in e-mail messages.

In this case, the Commission has obtained its

first ever Spam ban -- a ban prohibiting the defendants from ever again sending unsolicited commercial e-mail.

Moreover, on May 15 in Dallas, along with our Southwest Netforce Partners, we will announce new law enforcement targeting online fraud and deceptive Spam as well as a new initiative to address the pervasive problem of open relays.

Besides ramping up law enforcement, the FTC has disseminated informative, high-impact materials to educate consumers and businesses on Spam.

Our Spam website, www.ftc.gov\spam, has a wealth of information about how to avoid Spam, in the first instance, and what to do if you receive it.

Finally, our research informs our education in law enforcement. There seems to be more talk than actual knowledge about Spam. Thus, we conducted the remove-me surf to examine removal representations in Spam. We found that, contrary to the belief that responding to Spam guaranteed that you would receive more e-mail, 63 percent of the removal links and addresses in our sample did not function.

Additionally, in our Spam harvest, we examined how computer harvesting programs pick up consumers' publicly posted e-mail addresses, leading to more Spam.

In one instance, an e-mail address we used in a chat room received its first Spam message eight minutes after entering that room -- eight minutes.

From these findings, we could tell consumers what online activities placed them at risk for receiving Spam and what they might do to avoid it.

Yesterday, we announced another research effort -- the FTC Spam Study. In this study, we examined 1,000 Spam messages collected randomly from three sources: Our Spam database in the refrigerator; the Spam we received at the addresses used in the Spam harvest; and Spam that reached FTC employee computers.

We analyzed the messages based on the type of product or service offered, the indicia of deception in the content of the messages, and the indicia of deception in the from and subject lines. We found that 20 percent of the Spam contained offers for investment or business opportunities, including work-at-home offers, franchise opportunities or offers for securities. Eighteen percent of the Spam offered adult-oriented products or services.

Of these adult messages, about one-fifth included images of nudity that appeared automatically in the text. Further, 17 percent of the Spam involved finance, including credit cards, refinancing and insurance. Together the investment business opportunity,

adult and finance offers comprised 55 percent of our sample.

We also determined how many messages appeared misleading. Using evidence from past law enforcement actions and our own efforts, we identified specific representations likely to be false. We found that 40 percent of all of the combined categories of Spam messages contained indicia of falsity in the body of the message. An astonishing 90 percent of the investment/ business opportunity category of Spam contained indicia of false claims.

We also looked at evidence of deception in the from and subject lines of the Spam. One-third of the messages contained indicia of falsity in the from line. Messages falling into this category included from lines connoting a personal or business relationship, such as using a first name only or stating "your account."

Another common instance of misleading from line occurs when Spammers make the sender's name the same as the recipient's address, so it appears that you sent the message to yourself.

Additionally, we found that 24 percent of the Spam messages contained indicia of falsity in the subject line, such as using Ray to indicate familiarity or a subject line that was unrelated to the content of the

message, such as hi or order confirmation. Over one-third of adult content Spam contained false information on the subject line.

Adding up these various forms of deception, we found that 66 percent of the Spam appeared to contain at least one form of deception. Because we did not investigate the messages in the remaining one-third in detail, undoubtedly, at least part of it involves deception. Moreover, about 25 percent of this remaining one-third involves Spam for adult products.

This overall result is in sharp contrast to telemarketing, the overwhelming majority of which does not involve deception or pornography.

Additionally, even though required by several state laws, only two percent of the analyzed Spam contained the label ADV in the subject line. The picture this study paints is bleak. The overwhelming majority of Spam already appear likely to violate various laws.

Of course, finding and prosecuting these Spammers is a much more difficult task then simply categorizing the types of Spam.

To increase knowledge about Spam and to determine what role we might play in protecting consumers, we have convened this historic gathering. As you can see from the agenda, Spam affects many groups

-- marketers, ISPs, law enforcement anti-Spammers, bulk e-mail marketers, consumers and businesses -- both large and small.

We have planned three days of panels, discussing indepth virtually all issues related to Spam. The forum should provide useful information and help inform the public policy debate.

Day one will focus on the mechanics of Spam, will gather information on how Spammers find e-mail addresses and about the falsity involved in sending Spam. We will also learn about security weaknesses, such as open relays and open proxies.

Day two will explore the costs of Spam. We'll begin with an in-depth discussion of the economics of Spam. We'll then address more fully the cost of Spam to marketers, consumers, and new technologies. We'll discuss Spam blacklists -- that's practices for e-mail marketers and wireless Spam -- or unsolicited text messages.

Possible solutions to Spam will be the focus of Day 3. We will discuss state, federal and international legislation, law enforcement and private litigation and technological solutions to Spam. As you can see, we have much ground to cover.

Again, I'd like to thank the panelists for your

participation. We have 86 different panelists with a tremendous array of expertise. I'd also like to thank two of my colleagues, who I see are here, Commissioner Orson Swindle and Commissioner Mozelle Thompson, both of whom have done important work in the Spam area.

Commissioner Thompson will provide opening remarks for Day 2 of the forum, and Commissioner Swindle will open Day 3's discussion of potential solutions.

This morning we are also fortunate to have members of Congress with us, who are actively involved in this issue. And I'll introduce them individually before they speak.

Senator Conrad Burns, the Chairman of the Communications Subcommittee of the Senate Commerce Committee, has for many years focused his energy on the internet and the technology sector. Along with Senator Wyden, he has co-sponsored legislation to help curb the abuses of unsolicited commercial e-mail, which they just recently reintroduced this month.

Welcome, Chairman Burns.

(Applause.)

SENATOR BURNS: Thank you very much, Mr. Chairman. We appreciate the opportunity of coming down and visiting with you a little bit this morning on this important issue.

We started on this thing, I think, Senator Wyden, what, four years ago? So, welcome to catch up, folks. We try to look into the future and maybe try to get ahead of the curve on some issues, and this one was a tough one for the simple reason that four years ago or five years ago, as the figures would indicate, nobody really thought that this was a very serious problem. But, as time went on, I think, we see the merits of trying to get out in front of this thing.

I applaud the Chairman, this morning, for holding this important seminar or conference, whatever you want to call it, because I think it fills a vital void of getting some information out and airing some of the figures that we should get out and people be aware of.

I also want to thank Commissioner Anthony, who has supported Federal legislation and approach to this in the past and continues today, as we try to move some of the solutions forward.

I also want to know that in the final analysis, though, I still think it's going to take strong, legislative action in order to deal with this very serious problem. And I'll give you a little bit of background on me. I'm an auctioneer, I market, and I want you to know that anything that would curtail

marketing opportunities I'm sort of opposed to, but there's also a way to do marketing, and in the business world there is a way also and certain guidelines if you're going to be a professional marketer and carry on the world's business like it should be.

Let's face it folks, we live in an economic system where nothing happens in this system until somebody sells somebody something. We don't start any trains, trucks, cars or plants; we don't need electricity, we don't need anything until somebody sells something. And we don't want to limit that at all on the legitimate business world.

The Canned-Spam Bill would require emarketers to comply with a straight forward set of workable, common sense rules designed to give consumers more control over Spam. That's what it's all about.

And I want to publicly thank Senator Wyden from Oregon, because, I'll tell you one thing, he is a great partner, if he's on your side.

(Group laughter.)

SENATOR BURNS: If he's not, he's a worthy adversary, but he's undaunting, because, I mean, when he snaps into an issue, he stays there, like them old snapping turtles. And, so, we have worked on this a long time and he's just been relentless and I want to thank

him for his dedication to this issue.

Specifically, the Bill would require a sender of marketing e-mail to include a clear and conspicuous opt-out mechanism so that they could unsubscribe from further unwanted e-mail. Also, the Bill would prohibit emarketers -- e-mail marketers -- from using deceptive headers and subject lines.

I could go over and give you the rest of the figures, but the Chairman has already done that very ably and very capably, and put them down into numbers that we can relate to.

Canned-Spam includes strong enforcement provisions to ensure compliance; the Federal Trade Commission would have authority to impose steep, civil fines up to $500,000 on Spammers; this find could be tripled if the violation is found to be intentional.

The need for rapid action on this Bill is clear. The toxic sea of Spam has begun to engulf every medium of the e-mail. According to The Washington Post, of which, sometimes, we don't always agree, less than a month ago Spam currently accounts for 40 percent of all e-mail traffic and is expected to overtake regular e-mail in volume this summer.

While it's obvious to anyone with an e-mail account that the scourge of Spam has continued to worsen

the economic damage that Spam poses, paints an even more disturbing picture.

I just want to give you an example this morning on what can happen and what is happening in the real world. Sometimes we don't always live in the real world. Numbers are fine, but the true impact of Spam is seen in individual stories.

A constituent of mine, Jeff Smith, who built a fantastic fiber hotel in Missoula, Montana, has calculated that Spam costs his business over $300,000 a year. Nearly half of the bandwidth he buys is sucked up by Spam, and his company is only worth $2.5 million. That is real world.

The fact is that we've got to do something now and it has to have real teeth with real enforcement. The Bill that we have offered, Senator Wyden and I, as supported by pillars of the internet age, such as, YAHOO, America On Line and Ebay -- and Ebay is a wonderful organization, I will tell you. I use it a little, I flooded the market in spurs.

(Group laughter.)

SENATOR BURNS: I'm going to relate this little story to you, but I think this is legitimate. I've got an old friend of mine out in Montana that kind of, if you want anything in the world, he's got it. You know, one

of those junk stores and it's just piled up. Well, he's got baskets, bushel baskets and bushel baskets full of old spurs. And they were kind of tied together with batches and some of them got the rowels off of them, some of them broke the shank off of them, and this type of thing. And, so, I just went by there and I hollered at him and I gave him $5 for a whole string of these things and just throwed them in my car and you know how us men do, we get home and we hang it on a nail in the garage or out in the shop somewhere, and we don't ever look at it again.

Well, they must have hung there probably two or three or four years, and I got a friend of mine, I got this idea, because there was a couple of pairs of spurs in there and they were pretty good. But they were old, they had shown a little wear. And I just took a picture of this pair and I advertised them as antique spurs from Montana, put them on there. Them darn things brought $125 bucks.

So, I told my wife, I said, get the truck.

(Group laughter.)

SENATOR BURNS: And she said, well, how big a truck? And I said, we don't want to flood the market, just a small one, it will do.

But, clearly, I think we've got the clarion

call to do something about this, because, basically, those people who want to use the internet to market or even to tell other people about their product, there is a way to do it and a legitimate way to do it that the business world accepts and even the consumer accepts.

But what we're doing right now, we are killing a very tool that we use every day not only in the conduct of our business but also in our personal world. And we feel like now is the time to act on this particular piece of legislation.

Yesterday's New York Times editorial pretty much summed it up, and that's why we're here today and that's why we will continue to press. Last year, our Bill was cleared out of committee, it got to the floor, Senator Wyden did just yeoman's work on his side of the aisle, and I was working on my side of the aisle, and now we've got the same Bill this year, and now we'll move forward in the same way. And we think it's time to get it done and to get on with living and take some of this junk, like used spurs, out of our daily lives.

Thank you very much and, again, I applaud the FTC for this forum. It's very educational, but on the other hand, numbers are numbers, but right now we need to do something about it, and take action. Thank you very much and thank you, Mr. Chairman, for this opportunity

this morning.

(Applause.)

CHAIRMAN MURIS: Thank you very much, Senator Burns. I'd now like to introduce Senator Wyden, Senator Burns' co-author of the Canned-Spam Act. Senator Wyden is an outspoken advocate, he's extraordinarily interested in our issues at the FTC. I've spent many memorable moments discussing issues with Senator Wyden, and I'd like to echo Senator Burns' comments, because sometimes we agree and sometimes we don't. But it's my pleasure to introduce Senator Wyden.

(Applause.)

SENATOR WYDEN: Mr. Chairman, thank you very much, and let me say that the Spammers may not be quaking in their shoes this morning, because a Montana cowboy and a Jewish guy, who wanted to be in the NBA, are coming after them, but they sure ought to be.

(Group laughter.)

SENATOR WYDEN: I'm so pleased to be here with Chairman Burns. We have been part of a full-court press for the last three-and-half years on this issue, and I'm barely a household word in my own household, but to have Chairman Burns leading this effort and using his gavel as a bully-pulpit to mobilize support around the country is, I think, extraordinarily helpful and it is why we are

going to get this Bill on the floor of the United States Senate, because Senator Burns has made it clear he isn't going to give up.

He has said it so well, and I think I just want to make a handful of points, and I know you've got a busy program.

The first, it seems to me, is that the Spammers are not technological simpletons. And the challenge for our country is to try to figure out a strategy, a coordinated game plan between the public and the private sector, to try to stay a step ahead of them. And the reason I feel that way is my sense of what the Spammers are going to be like are sort of like sophisticated burglars cruising through a neighborhood. You remember what it's like. They, basically, go from door to door, kind of rattling at every single door, trying to find an opportunity where there's an opening. And when they find an opening somewhere, then they set up shop.

And, so, what we're going to need to do is to try to put in place a strategy for dealing with it. And let me outline what I think the three steps are for a coordinated game plan in terms of fighting Spam.

The first is, we absolutely must have, as Senator Burns has touched on, a top national law. The reason for that is if we allow a sort of crazy-quilt of

state laws -- and that's what I think is going to happen -- we're going to have a new state law practically every day -- we will have this hodge-podge of state statutes, there will be loopholes in them and Spammers will play the states off against each other.

So, point number one -- we absolutely must have a tough national law in order to do the job right.

Point number two is once we pass a tough national law, let's understand what the Spammers are likely to do. I think that the first thing they're going to do is try to move off-shore. I think it is very clear that if you pass a tough national law, they'll try to just go off-shore a little ways and try to set up shop there.

So, we are going to have to make it a priority in our discussion with our global commercial partners in trade and other areas to begin negotiations to try to close off those opportunities as a second part of this.

And, third, I want to make it clear that I'm of the view -- and I know Chairman Burns shares this as well -- that there is no way that you can pass a law that by itself is going to do this job. We absolutely must continue to fuel the engine of innovation in the private sector. And it's clear that that's what people in the Spam business are going to try to do, as well. They're

going to try to use technology and I believe that there are the brains and talent in this room and across the country to out-think and outsmart them.

But, in addition to the efforts to pass a tough national law, try to deal with the off-shore problem, we've got to continue to have your ideas and the technology innovation that comes from the private sector.

Suffice it to say, what this is going to be about is building a new partnership in the technology field. And Senator Burns chairs our committee -- I'm sort of his junior partner in this whole effort -- and what we have seen, as it relates to internet policy, is because there are no borders to the net and because the net and even communications on it don't really set down in a orderly kind of fashion, we're going to have to have new policies to deal with it, and I'm of the view that Spam is just the beginning of that challenge. We're going to have a whole host of other issues that are going to be presented with exactly the same kind of challenge.

So, it's important we do this right; it's important we do this right because the internet is still, with the digital divide, something that's pretty new to a significant portion of our people -- not everybody in this room, because you're probably on it a big chunk of the time -- but for a lot of Americans it's still a

pretty new medium. So, it's important that we set in place the kind of public/private partnership that's going to do it right.

Under Senator Burns' leadership, we will try to do our share, in terms of the Congressional level. We're thrilled that at a time when the country has been consumed by important issues of war and peace, that this issue has generated all of the attention that it has. And it really takes your breath away when you think about all that is going on in the world and what's happening, when legislators go back to their town hall meetings at home, people say, get that Spam! That's what happened to me last week when I was home, during a time when we're talking about the great triumph of our troops, citizens were coming up and saying, get after Spam; pass that legislation.

So, with your help we'll do it; with your help that will be the first step and, then, we'll move on to the other efforts that have to be undertaken to do this job right. We're really pleased that you're doing this, especially appreciative to the FTC for giving this attention the hot light that it deserves.

I'm of the view that as far as public policy is concerned, sunlight is the best disinfectant and that is what we're getting over the next few days, and we'll look

forward to working with you in the days ahead.

Thank you.

(Applause.)

CHAIRMAN MURIS: Thank you very much, Senator. Representative Zoe Lofgren represents San Jose, California and Silicon Valley. She serves on the House Judiciary Committee and the Cyber Security Subcommittee of the Select Committee on Homeland Security. The Congresswoman is planning on introducing her own Spam legislation this week, which I expect she'll mention in her remarks.

We are please to have her with us. Welcome, Congresswoman Lofgren.

(Applause.)

CONGRESSWOMAN LOFGREN: Thanks very much. I think this is an important conference today, and we all know that the flood of e-mail is a nuisance, but what we've learned recently during the last years, Spam is more than a nuisance, it's an economic burden.

Ferris Research tells us that U.S. companies will spend $10 billion this year because of Spam. And, in lost productivity, additional equipment. We've heard Senator Burns talk about the report that 40 percent of e-mail traffic today is Spam and that that will grow to a majority of e-mail traffic this year.

I'll confess that for many years, as the Spam Bills came before me in the House Judiciary Committee, I was resistant to a legislative approach. I have to confess that I said publicly, we have a delete button, that's all we need. But I think, actually, events have moved beyond that and the origin, really, of my reluctance to legislate is my belief that we should take a very light touch on the internet.

I am very concerned that we not regulate the internet, you know, it is a wonderful, free, open, standard medium that needs to be cherished and preserved, and we should always move forward with that in mind, but I'm also mindful that if we do not do something to deal with Spam, companies and ISPs are going to start changing the architecture of the internet in ways that we may not like to deal with the Spam issue.

And, therefore, I do think that a national law -- and I agree with Senator Wyden that ultimately we will need to have some international action -- is necessary. And, so, I actually am going to introduce a Bill later this week to Reduce Spam Act in 2003.

Now, I've got to give credit where credit is due, and that's to Professor Larry Lessig, at Stanford University, the author of many books on the internet, who got into a dare with Declan McCullagh from CNET, and

actually Larry Lessig dared Declan that if this Bill was introduced and passed and did not reduce Spam, that he would quit his job, and he believed that it would work that much. And, so, I actually took Larry up on that dare.

And what the Bill will do is actually to take a concept that has been adopted by many state legislatures and require that commercial e-mail do the ADV tagging. And what that, of course, would allow is to filter e-mail if you didn't want it. And thinking forward, you could also not limit it to ADV, you could do ADV 5 percent mortgages. So, you might also help sellers and buyers down the road to find each other as you further tag.

The interesting wrinkle on the approach that we are going to pursue is in the enforcement side. I understand that District Attorneys and U.S. Attorneys, basically, are not going to be taking a lot of action enforcing criminal laws about Spam. They are very busy dealing with terrorists and murders and muggers and they're not going to take up a lot of Spam prosecutions.

So, what this concept does is to allow for civil fines. We've already asked the FTC to devise the administrative procedure and, essentially, it gives a bounty to those who identify the Spammers. Up to 20 percent of the fine could be given to those who provide

the data that nails the Spammer in the FTC proceeding. And, in thinking ahead, we've got Spammers who are very clever. They are spoofers. But one of the elements, if you're selling something, is that you can find a way back to the Spammer, because they want to get your money.

And, so, whether they spoofed or not, I think they can be found and if we provide an incentive for those who are bothered by Spam to nail them with a 20 percent of the fine, I think we will have some enforcement.

Now, I'm busy, I will probably not participate in this bounty scheme, but I have an 18-year-old son who will. And, so, I really think of this structurally as unleashing the 18-year-olds to go after the Spammers, and I have confidence that American 18-year-olds are up to the task.

We will introduce this Bill later this week. I think it is an effective approach, but one that also respects the nature of the internet and continues to say we should not heavily regulate this wonderful medium, we should continue to have open standards and open communication.

Thank you all for being here today -- Spam is driving people crazy, and we need to deal with it. I think this conference is part of doing that.

Thank you very much.

(Applause.)

CHAIRMAN MURIS: Thank you very much, Representative Lofgren, and I'll now turn the floor over to Eileen Harrington, who is the Associate Director for the Division of Marketing Practices, who will begin with our first panel on Spam or further introduction to Spam.

Thank you very much.

MS. HARRINGTON: Thank you, Chairman Muris. If I could ask my colleague, Renard, to give me my papers, that would be really wonderful. And, I think, we now have all of our panelists seated. We have very little time for this panel, so we're going to jump right to it.

We want to set the stage for the rest of the conference by focusing on two things during our discussion -- and this will be a discussion, no opening remarks or speeches, and we'll cut you off if you do that.

But first we want to do some problem-definition discussion. And, then, I want to know from each of the panelists two things: I want to know whether you support Burns-Wyden; specifically, I want to hear your thoughts on the specifics of that Bill; and I want to know what it is specifically that the interest that you represent is doing -- and I want to know it in concrete terms -- is

doing or can do, right now, to reduce the volume of unwanted Spam.

But, first, let's focus on problem definition, and I want this to be in the nature of a discussion. So, I'd like us, as a panel, please, to throw out specific thoughts about what the problem is that we're talking about -- what is the problem? How do we define it?

Mark, do you want to start, give me a thought -- short?

MR. FERGUSON: The entire issue on Spam is whether or not it's solicited or not.

MS. HARRINGTON: Okay. So, solicited versus non --

MR. FERGUSON: Yeah.

MS. HARRINGTON: -- unsolicited?

MR. FERGUSON: Solicited versus nonsolicited. If you take into account that there are so many people that wish to sell something to you and that e-mail almost has a zero cost for the sender -- the recipient and the ISPs pick up almost 100 percent of the cost; the sender picks up almost zero percent of the cost. What is to stop the sender from sending to everybody? Nothing.

MS. HARRINGTON: So, key element, unsolicited. Bob?

MR. WIENTZEN: Well, to me the issue here has

been that the problems that we're facing are really being caused by a relatively small group of people who are committing fraud or in some way misrepresenting themselves or their offer.

So, for us, a key issue is identification of those who are causing the difficulty and vigorous enforcement of both existing laws and, hopefully, future laws which make it easier to prosecute those who are basically causing the difficulty.

MS. HARRINGTON: Bob, let me follow up on that, and we've worked together many times, so I ask the question with some respect, but with some edge.

MR. WIENTZEN: I expect nothing less.

MS. HARRINGTON: You guys always say that the problem is caused by the fraudulent few. You always say that, but I'm not sure that -- notwithstanding the findings in the study that we announced yesterday -- that it's just the fraudulent few. How can you support that?

MR. WIENTZEN: Well, first of all, in the last six months, we've met with some 250 folks in the industry -- experts, many of the people in this room, and representatives of their company -- I think the overwhelming view of that group is that the problem is caused by relatively few. The number 200 serious Spammers and companies causing a great deal of this

difficulty has been mentioned.

We've met with the top people --

MS. HARRINGTON: What's the backup on that 200? Do you know?

MR. WIENTZEN: Well, I can give the names of the folks, for example, at the Justice Department who site that number. The FBI cites a number similar to that.

While there are hundreds of thousands of probability of individuals who are causing the Spam problem, there is a huge volume coming from a relatively small group of folks or companies -- under many names, under many identities, and so forth -- and we think we need to have a very, very vigorous effort underway to root those people out. Getting them identified would be a great start, and that's one of the things we like in Burns-Wyden, we think we have to have a real forceful way to cause people to not only identify who's sending the message but physically where they are. And if they lie about that, that is an easily prosecutable kind of a thing.

So, the sense that we get is that if we could take the big, you know, the 80 percent/20 percent rule, if we could get at the people who are causing 80 percent of this problem fairly quickly -- and we are encouraged

by the fact that there are not hundreds of thousands of people accounting for the 80 percent of the problem. And I think you'll find the same.

And, frankly, I read your study on the way down last night, and I think it backs up what we're saying, Eileen. Tremendous volume has really gotten very evident problems under existing law. Not that we shouldn't have more laws; we think we should; but let's go after those people who we can get now, and you need help, the Justice Department needs help, the FBI and the Secret Service needs help.

I continue to feel that a country that can conduct an operation that we just conducted and cannot deal with a Nigerian scam problem is ridiculous. I mean, how can we let that problem continue to go on, year after year, and not solve that, while we've worried about somebody who might be operating from their basement, selling computer printer cartridges?

Let's go after some of these people who are dumping hundreds of millions of Spam e-mails in the system and get them and get them now.

MS. HARRINGTON: Okay. We're really pleased to have The Honorable Christine Gregoire, Attorney General of the State of Washington, with us. She has been on the front lines and a leader, both, on this issue in the

states.

Chris, what do you think about what Bob Wientzen just said about the bad few versus the mass marketing?

MS. GREGOIRE: Well, respectfully, I would suggest that it's far more difficult than what has just been portrayed. For example, in the State of Washington, alone, a year ago in the month of February, we had approximately 700 complaints with respect to Spam from consumers in our state. One year later, we have 1,700, and in one case alone it took us 14 pre-suit subpoenas to try and identify who really was the Spammer that originated the action in the first place.

So, it isn't, in my opinion, just a few, and it's extremely difficult, and the cost to consumers is not only a waste of time, but also the fact that they are very concerned -- and we get this complaint constantly -- about what is being portrayed to their children by way of pornography that is uninvited into the home and they can't get it out; the results of which is, I would say that we've got a significant problem on our hands and we're only going to be able to do it if we do one thing and that is enforcement.

Two, we've got to have technological advancements. ISPs are doing a fairly good job, but

they're having difficulty getting out in front of the Spammer. How are they going to be able to filter out? How is the individual consumer, from a technological basis, going to be able to filter out when they chose to do so, particularly on the new pop-up screens that really are very capable of getting around the consumer's ability?

So, I think we're going to have to have a view towards the future, on behalf of consumers, that says, yes, enforcement, technology advancements, capability by ISPs, and, yes, legislation -- but I will hold my remarks until later, but we, the Attorneys General of this country -- and 44 of us notified the sponsors of the Bill yesterday -- have considerable concerns about the pending legislation before Congress.

MS. HARRINGTON: Thank you, Chris. Let me just recap where we are on our discussion here in flagging key elements.

Unsolicited -- we have one view that the problem is the few large bulk mailers who are fraudulent.

We have the point made that a key part of Spam problem and the definition is that it's very difficult to identify the senders.

And, Attorney General Gregoire adds an important point that their technology use is ever-

changing and we're now into pop-ups.

Let me just say that we're not introducing our panelists because you all have their bios and we really want to get to the meat. So, that's why we're not spending time on the fluff, but -- or the meat, if you will --

(Group laughter.)

MS. HARRINGTON: Joe Barrett from AOL, what can you add to the problem definition discussion?

MR. BARRETT: I think it's really important that we consider how large the problem is. There's just a flood of complaints out there of Spam out there. We've hit as many as nine million complaints a day -- and that's coming against large volumes of mail, different kinds of mail. Ultimately, the decider of Spam is the person who receives it. When mail is received by someone and they don't want it, they know it. It's really obvious when it shows up.

MS. HARRINGTON: Okay. So, volume is a very key element in the definition. I'd like to ask -- we have someone who's in the business of doing bulk e-mail marketing, Thomas-Carlton Cowles. What do you have to add to this discussion?

MR. COWLES: I think that what we need is accountability. We need some way that e-mail can be

watermarked, if you will, so that people can be tracked and people should be registered to send e-mail.

MS. HARRINGTON: Let me flip it then. So, what you're saying part of the problem is is that there isn't accountability?

MR. COWLES: Correct.

MS. HARRINGTON: That's an element of the problem. How are you accountable, if you are? I mean, some would say, ha, you know, you're sending out a lot of this stuff.

MR. COWLES: Well, any person that is a responsible marketer, has self-accountability and they're trying to do, you know, the right thing when people ask to be removed or to be joined to a particular list. And, I think, what we need is a place where we can go to the FTC and register as a publisher and an end-user could block your publisher license, if you will, that would be included in the e-mail that is sent out.

MS. HARRINGTON: So, lack of accountability, lack of government-sanctioned means to enforce accountability, those are two problem elements?

MR. COWLES: Yes.

MS. HARRINGTON: And right now, in the meantime, we're just relying on your guys to examine your consciences?

MR. COWLES: Well, not only that, but you also have the ISPs are charged with the task of deciding what is real and what isn't real, and they're filtering out things that are very valid, like a message to your wife, or a message to, you know, someone you care about, is getting filtered, and that's a problem.

MS. HARRINGTON: So, another element of the problem is that, right now, on this accountability issue, there isn't a reliable way to filter out without being over-inclusive?

MR. COWLES: Absolutely. I mean, it is an extreme problem, and we do have -- the volumes are increasing -- and that is a problem, and it does need to be stopped. I actually have a flow chart, if you want to look at it.

MS. HARRINGTON: Okay. And we'll put that in the record, as well. Thank you.

All right, now, Clifton, you run a relatively small ISP lava.net. From your perspective, what do you have to add to this growing list of definitional elements?

MR. ROYSTON: From my standpoint, there's two aspects of the problem with Spam: There's a huge cost to systems, the actual operations of an ISP on the internet -- which I'm surprised Joe Barrett didn't speak to.

There's also a huge cost to people -- the recipients in terms of their time -- opportunity costs, time spent that they could be doing something constructive that they're spending deleting Spam. And, really, the loss of human time is the biggest cost factor for the ISPs, the amount of staff they need to deal with upgrading servers, operating things, but also for the individual recipients.

My estimate -- and I tried to come up with for this conference -- is that as a small ISP it costs us somewhere between $150 to $200,000 last year just dealing with the Spam problem. That includes mail server upgrades, staffing, loss of customers -- people cancelling their accounts to switch to a new address because of the Spam they were getting -- trying to develop some kind of inhouse Spam filtering system that would not lose important mail -- which is a weakness of some systems -- tremendous number of tasks and costs that we had just dealing with this problem, and that's reflected in everyone's internet bill. What it comes down to is a large portion of the bill you're paying for internet access is now accountable to Spam, because they are costs that your net provider is incurring to deal with the problem.

MS. HARRINGTON: Clifton, how much Spam comes through your system every day, do you think?

MR. ROYSTON: I'm not tracking the total numbers for our system as a whole, but on certain mailboxes, basically, my own mailbox, which gets things from a number of alias that I use as kind of a benchmark, it jumped from about 100 a day, as of December -- November/December last year -- up to about -- between 350 and 400 during March; and, then, April, as of the point that I left, seemed to be showing roughly a 50 percent increase over March.

So, the reports that were talking about a 50 percent increase in Spam by the end of this year, were wildly and naively over optimistic. We've seen more than four-fold increase already this year, and it's going up 50 percent month-over-month at this point.

MS. HARRINGTON: Okay, so, exponential growth in volume to add to Joe's volume point on the definitional list.

MR. BARRETT: Could I add just a little bit on the volume?

MS. HARRINGTON: Sure.

MR. BARRETT: When we look at volume, it's hard to tell how much of what gets delivered is Spam for certain. We do a huge amount of filtering on inbound mail. Recently, this week, we blocked 3.27 billion -- with a "B" -- pieces of mail. That's doubling in a

period of eight weeks. A huge amount of mail.

If that mail had arrived in, like envelopes, and we had taken these and laid these end to end, they'd go around the globe four times and reach onto the moon. That's how much Spam we stopped in a single day. Of course, our members would love it if we would just send the Spammers up there along with the mail -- Spam, that is.

MR. WIENTZEN: Eileen, could I add something to your list?

MS. HARRINGTON: Sure.

MR. WIENTZEN: I think we need a definition of Spam that works, and we've been trying very hard to come up with that. I think we have to respect the Constitutional rights of everyone and we have to also, I hope, preserve the rights of marketers to use this tool. So, we would submit it's something along the lines of bulk commercial e-mail which does not have an honest subject line; which does not have an accurate header and is perhaps forged; which does not have the complete ID of the sender, including the sender's physical address; and does not have an opt-out that works -- an easy-to-find and easy-to-implement opt-out that works.

We would submit that opt-out that works has to be in every single piece of commercial e-mail.

MR. FERGUSON: Can I respond?

MS. HARRINGTON: Hold on, because we haven't heard -- and you'll be able to -- but I want to hear from Laura and I want to hear from Brian.

Laura, you are both sort of an activist from the consumer side on the Spam issue, but you also, now, are a consultant working for companies that are using e-mail.

MS. ATKINS: Yes.

MS. HARRINGTON: So, tell us what you would add to this list and tell us what more consumers could be doing right now that they may not be.

MS. ATKINS: I would go back to the problem with Spam is that it's unsolicited and that it's sent in bulk. And this is the definition that both in the business and as a advocate for SpamCon Foundation we use.

MS. HARRINGTON: Okay, so you wouldn't add Bob Wientzen's "and there's something deceptive in the header?"

MS. ATKINS: No.

MS. HARRINGTON: Okay.

MS. ATKINS: Because the deception does not mitigate the problems with the bulk going into places like lava.net and into places like AOL and into your ISP account.

MS. HARRINGTON: Now, let's just do a quick check to see where our panelists are, and that's a fundamental issue, and I'm going to let you finish, but how many agree with Bob Wientzen that a key part of the Spam definition is deception? How many agree with Bob except Bob?

Hands? Bob and Thomas and Christine. So Spam is not just bulk, not just unsolicited.

MS. GREGOIRE: I want to go back to the Constitutional issue, for just a brief moment. I think you can declare it illegal and go out and do whatever you want to do by way of civil penalties and ultimately, potentially, as Virginia did yesterday, criminal, but only if it's unfair, deceptive, what have you.

If you want to regulate it, then I think you can do precisely what you're talking about. But I would split the two and talk about them and understanding they have to be overlaid on the context of the First Amendment.

MS. HARRINGTON: Okay. Laura?

MS. ATKINS: I would agree that there are different definitions of Spam for different fits. An ISP, like AOL, is free to define Spam coming into their network as things our users don't like. At SpamCon Foundation, we're looking at a much broader constituency,

so we don't define it by what you don't like but we define it in the broader scope of unsolicited and bulk.

In terms of regulations and laws, there are some issues with the First Amendment and, so, unsolicited and bulk may not be the best definitions for a law.

MS. HARRINGTON: Okay. Thank you. Now we're saving the biggest for last -- or maybe the biggest, I don't know. Brian?

MR. ARBOGAST: Yeah. So, I think that Spam really is about, what does the user think? Is this mail unsolicited? Is it unwanted? Is it bulk e-mail? And, as Joe mentioned, you know, we already -- at Microsoft, at MSN Hotmail, are also filtering, you know, billions of e-mail messages -- it's an astounding volume that's growing at an astounding pace -- but what's key is to provide the tools to give users more feedback over what's legitimate and not legitimate e-mail.

So, for instance, I think thinking of Spam as just one bucket is probably inappropriate. You have your clearly fraudulent and deceptive e-mail; that's one kind of unsolicited bulk e-mail. But there's also an opportunity, I think, for us to define what is really best practices as a marketer.

We talked about, you know, marketing has a value, but there's a way to do marketing right. And, I

think, there's an opportunity to set some very high bars for what a legitimate sender does, in terms of not only whether they respect unsubscribe links, but also how do they get their e-mail accounts in the first place? How do they get consent from the user? And if we could give a way for the legitimate senders to step up to a set of principles that then could be reliably associated with the message, then all of a sudden Joe's filters, my filters -- every ISPs filters -- could do a much better job of differentiating the legitimate senders, who are doing their best, because frankly they care about their brand and they care about the customer relationships. The filters would treat them somewhat differently than they treat the unwashed masses, which would be somewhat different even from anything that's very clearly, from a filter's perspective, fraudulent or deception. In other words, something that clearly is coming from an IP address other than what the sender should be sending from.

So, I think that there are ways that we can differentiate -- and I think legislation can also help us define this category of best practices -- not necessarily by codifying what the best sender guidelines are in a law that may not change for years -- but I think there's an opportunity to provide a model for a safe harbor in

legislation that would look to an independent authority, in the private sector; a nonprofit authority that could, on an ongoing basis, keep up with the times and keep up a definition of best practices, because we all know that the Spammers evolve day to day to be more effective.

And maybe the way to kind of get some teeth around that -- how people can flock to that best practice -- is to have it married to an ADV labeling approach, where if you either step up to a set of best practices or you label your unsolicited commercial e-mail with an ADV, that kinds of gives you really a broad approach that will help the technology do a better job of filtering; that will help users understand these different categories of e-mail; and, I think, really is the marriage -- kind of a coordinated game plan that Senator Wyden talked about -- it has technology, legislation, enforcement and consumer education all coming together to solve the problem.

MS. HARRINGTON: Okay. Thanks. Mark?

MR. FERGUSON: Well, I was going to talk to Mr. Wientzen's comment about the Constitutionality of marketing.

Advertising is not Constitutionally protected speech. It doesn't share the same Constitutional privilege that the general populace has with regards to their freedom of speech, because the spirit of the

Constitution, the First Amendment, was towards presenting ideas -- different ideas -- not trying to sell something.

So, it's kind of a different issue whenever you attempt to veil marketing and theft -- which is what Spam is -- as a Constitutional guaranteed free speech. It's not the same thing.

MS. HARRINGTON: Well, that's an issue that's very much in contention before the Supreme Court right now, and one that certainly carries through this discussion.

MR. FERGUSON: Rehnquist already ruled on it. No matter the merits --

MS. HARRINGTON: He only has one vote the last time I checked.

(Group laughter.)

MR. FERGUSON: Well, this was a ruling awhile back. Rehnquist ruled -- it was somebody suing the USPS -- a marketer -- and Rehnquist already ruled on that case. His comments after were, "No matter the merit of the speech, no one should be forced to accept delivery on it or to be forced to receive it." And that was his ruling.

I can get that and get it to you, so that you can see it. It's an actual citing of a case.

MS. HARRINGTON: Okay. Well, thank you. I

think, though, that what we see is that part of, when we are looking at definitional elements, there is -- in the problem definition -- a certain tension around speech issues that is just there -- it is there.

Clifton?

MR. ROYSTON: Yeah. I just wanted to say that I think, to me, the key aspects of the problems of Spam are the combination of this factor that it's unsolicited and that it's bulk, as Laura mentioned, and the reason those two go together to create a problem is that that combination means that there's an inherent difficulty for the recipient in managing it.

If you're getting an unsolicited e-mail from a particular individual, then that's not a problem for you, typically. But if you've got 10,000 individuals, each sending out 10,000 messages to 10,000 different people per day, no matter whether those messages are fraudulent or not, the recipients are going to have a problem with the sheer volume, and that's something where it's true that what Robert Wientzen said, the bulk of the problem, right now, 90 percent of the problem may be coming from a small number of frauds and con-artists, but when that 90 percent is removed, the 10 percent that's left already is going to be a bigger problem Spam than we had five years ago. And that remaining 10 percent is going to grow.

Yes, let's address the 90 percent of the problem that's there now, but let's not do it in a way that then bars us from dealing with the remainder of the problem. That's my big concern about legislation is that it not be worded in a way that blocks us from addressing the remaining parts of the problem we don't yet fully agree on.

MS. HARRINGTON: Okay. I'd like to move the discussion now off of the definitional point and on, specifically, to Burns-Wyden, which is the piece of legislation that's been pending out there for the longest period of time, and I want to know from each of you what your position is on each of the key aspects of the Burns-Wyden Bill -- support, oppose, and very concisely why. And I'm going to sort of be a bit of an autocrat on the concise issue.

Brian, where are you guys?

MR. ARBOGAST: We think it's a good first start. We think that some aspects of it need to get strengthened. We would like to see, for instance, road blocks to ISP enforcements removed.

MS. HARRINGTON: What are the road blocks?

MR. ARBOGAST: My understanding is not strong enough opportunity for ISPs and state agencies to enforce --

MS. HARRINGTON: So, private right of action and state right of action?

MR. ARBOGAST: Yes. And I'd also say that adding this combination of ADV labeling will provide safe harbor for promoting best practices and sender guidelines would also be a tremendous addition to the Bill.

So, I was just saying, I also think that giving states' ISPs a private right of action is one way that I'd love to see the Bill strengthened. The second way would be to introduce this concept of ADV labeling along with a safe harbor mechanism for industries to define best practices for commercial e-mail senders, and have that be a safe harbor.

MS. HARRINGTON: Why hasn't the industry done that already? I mean, why should people take comfort in a statute, as you outline it, that gives industry another bite at the apple?

MR. ARBOGAST: Yeah, I think that there's been a lot of talk, but it's been fragmented so far. To be honest, I think, this conference alone has driven a tremendous amount of discussion in the past couple of months as to what are best practices in the marketing world, and I think some centers probably hope that this wouldn't become a problem they'd have to deal with, but the false positives that we're seeing as we introduce

filtering capabilities as the only way to protect consumers' mailboxes, that's leading to direct marketers now worrying that, while they need help for e-mail to remain a viable business for them, even if they're stepping up to the highest bar in terms of best practices.

And, so, I think what you finally have now is both the senders and the ISPs -- and I think many people who are thinking about legislation -- realizing that best practices that can keep pace with the times and that are supported with, you know, some independent authority that can help to dispute resolutions, et cetera --

MS. HARRINGTON: Brian -- thank you. Chris?

MS. GREGOIRE: Well, last evening the State Attorneys General forward onto the legislators a very clear message about how we felt about Federal legislation in this area. And this includes 44 State Attorneys General raising the concern about pre-emption. Why would we pre-empt state laws when we don't have a tough enough, overall, Federal proposed legislation, is the fundamental question.

I don't think Attorneys General will oppose an overall Federal piece of legislation so long as it's tough enough. But that which is being proposed is not, in our mind, sufficient in order to protect consumers.

MS. HARRINGTON: How could it be strengthened in a way that would cause the AGs, in your mind, to drop their opposition to pre-emption? What would it take?

MS. GREGOIRE: Consumer protection laws begin by displacing the elements of fraud in law, and this Bill, unlike anything we've seen in a long time, reinstitutes the elements of fraud rather than simply saying, consumer protection laws are the law of the land. Why in the world we would give more credence to Spam and a more onerous responsibility for those who enforce in this area, is beyond us.

So, we think the elements of intent and materiality and so on ought to be eliminated and you ought to put back basic consumer protection laws of the respective states and the FTC, as well, by the way.

Secondly, the defenses are far too many. Why are we allowing the defenses in this particular instance that are unlike others; for example, if it's an opt-out and their mailbox is full, then that's a defense.

Well, sorry, my mailbox is full of their Spam and that's not my defense.

(Group applause. Bravo, bravo.)

MS. GREGOIRE: So, we would suggest the defenses have far too many loopholes. The bottom line is we also think consumers have to have a private right of

action. Why, in this area, have we decided to say to the consumers, we are making your life miserable; we are costing you money, but, oh, by the way, you have no recourse; it's up to the FTC, the State Attorneys General and whatever the Federal Government may say by way of Federal legislation.

So, the bottom line is, it's a good start. I'm not going to suggest it's not a good start, but there's a long distance to go. We're ready, willing and able to work with these respective Senators and Members of Congress in order to make it effective and efficient and get this onerous burden off our consumers and off our good businesses today.

MS. HARRINGTON: Thanks, Chris. Bob, I bet you have a different view.

(Group laughter.)

MR. WIENTZEN: You better believe it. You know, with all due respect, I think if we become emotional and irrational here, we're liable to throw out the baby with the bath water, and I think we want very much to avoid that. We think the Burns-Wyden Bill is absolutely the way to go in principle, and in approach I think we have some very small, technical niggles to deal with it, but we are supporting the Bill and have been for a long time.

I think we need to get on with it. I think we need to pass a Bill that will enable more effective and, I think, much faster enforcement than we're going to have if we spend another year or two trying to come up with something which will answer all of the problems.

Let's face it, by the time the government figures out how to get a bill that enables with, in her opinion, all of the problems, the problems will be very different -- that's the name of the game here.

So, we want to get on with it, we think Burns-Wyden is the way to go --

MS. HARRINGTON: You're supporting it in its entirety?

MR. WIENTZEN: There are some technical issues, and I think the staff recognizes -- and, I mean, technical niggles -- in the bill, but, yes, we are supporting the fundamentals of that bill, which we think should have been passed last year, frankly.

And, then, providing enough money -- be it to you or someone else, Eileen, to go out and enforce it. I mean, it's not going to do us any good to continue to add more legal actions here if nobody goes out and enforces them.

Now, I think it's very easy to get very emotional about having consumer protection, but you've

got a significant part of the American economy that is, in fact, being spurred on and growing as a result of being able to use e-mail.

We did a study just this past Monday -- 37 percent of the folks we talked to on a nationally represented sample, said they had bought something as a result of receiving some e-mail. That's not inconsequential, and it is growing. You know, everybody doesn't hate all e-mail. Most of our members --

MS. HARRINGTON: Now, Laura, would take a different view.

MS. ATKINS: No, actually, I would agree, but I would say that the majority of what they're buying and the majority of the people in your study are not buying based on unsolicited e-mail, that they're buying based on solicited mail. And that to lump all unsolicited and solicited commercial mail in the same pot is confusing the issue and is making it more difficult for people to sort out the problems versus the good bits. And I don't think anyone here wants to actually stop solicited commercial e-mail. I certainly don't. That's a part of the medium and that's part of what SpamCon wants to do is keep e-mail as a viable communications medium, and that includes from business to consumer.

So, I don't think you can say that that 36

percent is people buying based on unsolicited bulk e-mail.

MR. WIENTZEN: Yeah, but, Laura, there wouldn't be any solicited e-mail if there wasn't some way to approach these people, unless you see the future --

MS. ATKINS: There are a number of ways to select e-mail addresses --

(Group boos.)

(Group laughter.)

MS. HARRINGTON: All right, now. We've got everybody juiced without even having coffee. Let's hold that -- and Clifton says that's wrong, Bob.

MR. COWLES: This is something that I think is really being missed -- the DMA is actually serving its constituents, its members, very poorly here. Let me give you an example of some things I buy out of the solicited commercial e-mail I receive. I subscribe to the BMG Music Club; I subscribe to the Science Fiction Book Club; and you know what? I have a hard time finding the solicited mailings that I'm asking for from those companies because they're either getting drowned out in the hundreds of Spams I receive per day, thousands per month, or they're getting caught mistakenly by the Spam filters that, even as I've done my best job as one of the developers of them, to tune them, it becomes very hard to

distinguish the good, valid, valuable commercial e-mail from all the junk that's pretending to be good, valid, valuable commercial e-mail.

What's more, another of things or catalogues that I want, I get an e-mail, the people voluntarily put the ADV tag on it and, you know what? That just causes it to get lumped in with the rest of the Spam, too.

So, the labeling, as it stands, is not an adequate solution. It's going to further harm commercial -- genuine, legitimate commercial marketers sending soliciting e-mail by causing it to just get lumped in with all the Spam.

MS. HARRINGTON: So, you oppose that aspect of Burns-Wyden?

MR. COWLES: I think the labeling is too broad a brush. I agree with Brian that labeling is a potentially valuable solution, but there needs to be some kind of finer grain labeling because if every piece of Spam that comes in says ADV, it doesn't help me to sort out the Spam from the real commercial e-mail.

MR. WIENTZEN: Burns-Wyden doesn't have labeling.

MR. COWLES: I'm sorry. But, in general, I really have to agree with most of what Christine said. It's a bad idea for Federal legislation to be pre-empting

stronger local or state legislation. I mean, if we have Federal laws against fraud and against various categories of armed robbery, bank robbery, those don't prohibit the states from also having their own laws on the books against criminal acts.

MS. HARRINGTON: Okay. Thank you. Mark?

MR. FERGUSON: Oh, how are you doing? I don't think you are emotional. Hey, Bob, I've got a question for you. You realize, of course, that the bulk mail industry, whom you represent here, is subsidized by first class mail?

MR. WIENTZEN: No, I don't recognize that, but go ahead.

MR. FERGUSON: Well, that's a common known fact, it is, bulk mail is subsidized by first class mail.

MS. HARRINGTON: Let's get to Spam here.

MR. FERGUSON: Okay. Now, with the subsidizing that goes on with the regular mail system, it's only a small percentage, but the subsidizing that you're proposing to make legal with this Spam legislation here that you're putting, would put at least a $2 a month cost to each end-user in the United States. AOL has 30 million end-users.

MS. HARRINGTON: So, Mark, you don't support Burns-Wyden for one reason?

MR. FERGUSON: It legalizes Spam.

MS. HARRINGTON: Okay.

MR. FERGUSON: Spam is actually -- a good definition of Spam is forced advertising. The way that the e-mail system works is the server receives the package and the ASCII files are written to the server and in order to remove those files from the service, the user is forced to download them. And that's forced advertising. And that, to me, is wrong. And, then, you want the user to, again, pay for that forced advertising. And AOL is passing along approximately $60 million a month to their end-users at $2 a user.

MS. HARRINGTON: Okay. Thomas?

MR. COWLES: Well, I can actually touch on that point he's talking about -- forced to download. And I also heard about identifiable -- making things more identifiable, and I do agree that things need to be more identifiable, which is why I think the Federal Trade Commission could be a place where you could register an identity and include that in the header of the e-mail that they send out. And that would allow a consumer to, basically, read the header without downloading the message or the ASCII file and deleting it before they actually download it.

So, that would solve that problem, and it would

also give people the ability to create third-party software because this publisher ID system would be in the header. And a consumer would make those choices and I think this is a good first step, definitely. But we need to use technology as the solution to this problem.

MS. HARRINGTON: You have a question, Laura?

MS. ATKINS: Why was Empire Towers not establishing this just outside of just going ahead and deciding they're going to global all of their mail and allow the consumer to make those decisions without an action by the FTC?

MS. HARRINGTON: Speak in the mic, please.

MS. ATKINS: Why has Empire Towers not gone ahead and done this and labeled their outgoing e-mails in the headers without waiting for FTC action?

MR. COWLES: Well, we're not here to discuss, you know, my company. I think this is more discussing the issues --

MS. HARRINGTON: Oh -- I'm not sure.

(Group laughter.)

MR. COWLES: -- and I don't --

MS. HARRINGTON: I think we're here to discuss very specifically what the stakeholders are doing and not doing.

MR. COWLES: Well, yeah, I do agree, but I

think that we don't have enough clout in the industry or in the ISP world to, basically, propose these technological solutions, and this is why I think it's a great time to actually talk about it. And I'm glad that this is finally happening and I wish it could have happened sooner.

MS. ATKINS: But there was nothing to stop you from labeling your mail in the headers, already?

MR. COWLES: We do label everything.

MS. HARRINGTON: Okay. On Burns-Wyden, we haven't heard from Joe.

MR. BARRETT: We've worked with Senators Burns and Wyden on this. There are some important elements in it that I think are good. It sets some good baseline behaviors for, basically, the good actors, and that's a good thing.

It needs to be complimented, though, and it's important that it be complimented with strong criminal penalties for the really slimy folks. It's not good enough to have the good actors behave better, getting the real bad actors nice little rooms where they can stay for a few years, that has a lot more impact. The kind of law that we have in Virginia that we just signed, I think, is a good example of a law with some teeth.

MS. HARRINGTON: I have a quick question for

the ISPs. We'll start with Brian. Do you block IP addresses that send Spam?

MR. ARBOGAST: Yeah, we do a lot of things to try to identify Spam, and looking at IP addresses is one of the ways.

MS. HARRINGTON: And you block them?

MR. ARBOGAST: And we block it.

MS. HARRINGTON: Joe, do you block IP addresses?

MR. BARRETT: We will block IP addresses when we have complaints or we have confirmed bad characteristics, like open relays, open proxies, open routers, that's right.

MS. HARRINGTON: How often does that happen, do you think?

MR. BARRETT: Dynamic addresses is another example. It happens all the time.

MS. HARRINGTON: Clifton?

MR. ROYSTON: We couldn't survive without it. I mean, the numbers I quote on Spam are after using multiple blacklists to block many addresses from even delivering mail at all to our servers and, then, we use additional blacklists, which are less 100 percent reliable as part of our filtering system, after we've accepted the mail, to filter it at the user's discretion.

MS. HARRINGTON: Okay. Thomas, what specific steps are you taking at your company to avoid overburdening ISPs with your marketing campaigns?

MR. COWLES: Well, we primarily stick to whatever proposed legislation, as it changes on a day-to-day basis, and the atmosphere is ever-changing and that's why we support Federal legislation so that it's something that we can follow. And our subscribers are opted-in and opted-out as they choose.

MS. HARRINGTON: Okay. Bob?

MR. WIENTZEN: Eileen, I wanted to comment on Brian's discussion earlier of some way to provide some sort of status for those who are providing a glaring and appropriate view of the best practices.

We think this is an approach that could work and we've been working hard and talking to a number of folks. There are some legal challenges that need to be dealt with. We've calling it the gold list or some people are calling it the white list. With the exception of the comment that Brian made about labeling, which we think has some real problems, we think that having this best practices concept, signed onto by companies or individuals, and then having the ISPs be aware of that and use that in making decisions, we think might be a way to make it easier for those who are following the high

standards, to do the job that has to be done, to continue to be able to market using e-mail and, at the same time, have those that are doing offensive things not have the forum that they have at the moment.

We think that can be done and, at the same time, it might be a way to put some economic penalty in, which I know folks would like. We think there's a way to do that.

So, we are hard at work at that and involved early-on some of the companies that are here and we expect in the next few weeks to have agreement on it -- at least what a framework for what that would look like.

MS. HARRINGTON: I would be, I think, remiss in my job of facilitating the panel if I didn't just give voice to a thought that probably many are having; which is that it could be that best practices are like fiddling while Rome is burning.

MR. ROYSTON: We don't think it's the whole answer, Eileen. We absolutely agree with you on that, and we think a lot of the problem here has been that there's been a lot of talk and no action, and we think the time has come for some action, be it action that is not likely to be the silver bullet that everybody wants. We're not going to stop it all, but let's stop the big chunk of it and let's stop it now.

MS. HARRINGTON: Well, let's turn back to Chris for just a moment, where there has been action. The State of Washington has a Spam statute, you're responsible for enforcing it. I know that your resources are very limited, too. The states are particularly strapped right now, but that said, how effective is the Washington Spam law? Do you have anything that you can tell us about measures, about experience, has there been a decrease in the wake of the State v. Heckel decision, has there been a decrease in Spam, do you think, in Washingtonians e-mail boxes?

MS. GREGOIRE: Well, I'll give you a bit of an ambiguous answer here. We were the second state to pass legislation and we passed it in 1998. We were very careful in doing so with respect to the First Amendment and made it very clear that it had to be misleading header and so on and so forth, as well we should have in light of the fact that we challenged all the way to the United States Supreme Court, and ultimately the holding of the Washington State Supreme Court there was, interestingly enough, while the First Amendment does protect commercial free speech -- not as much as speech that you and I may have, by way of protection -- it does not protect somebody from lying, somebody misleading a consumer, which is exactly what happened in the State v.

Heckel case. We have now imposed in that case $98,000 in fines and penalties, attorney's fees and costs, and that is now on appeal.

The fact of the matter is, because of that case, and because of the challenge that went up to the United States Supreme Court, I think we have more consumers complaining today. They were not complaining yesterday because they were just frustrated and didn't feel there was anything they could do.

So, if the measure is are we getting complaints? We clearly are. And, so, that would suggest that maybe the problem is getting bigger rather than smaller. I simply think that's a frustrated consumer, who has had it -- and, yes, I am passionate about consumers, and I do not apologize in any way about being passionate about their frustration, but I think they are so frustrated now by the volume that you all are referring to, and -- by the way -- they're looking to us to see if there isn't something that can be done.

At the end of the day, I think, basically, our law is too new in terms of enforcement, because we just had it declared Constitutional, and now we're in the process of enforcing it, but we are hampered by our own physical constraints, and that's why I think at the end of the day you will find state AGs saying to you, it's a

partnership here. It's a partnership with the consumer, who has resources available to them and private right of action; it's law enforcement doing what they can, particularly with regard to the very bad actors, and giving us criminal enforcement over them; and, yes, it's giving sufficient leeway to ISPs and others to come up with new, innovative, technological ways in which to address this issue that will be at the end, probably far superior, to any piece of legislation, state or Federal.

MS. HARRINGTON: We have heard, in this opening discussion, I think, some of the key points of difference that we are going to really plumb over the next three days. We are nearly out of time. Let me just make a couple of remarks.

First, on future panels, there will be an opportunity, we hope, for your questions and also questions coming in by e-mail. We are, you know, sort of -- not Spam.

(Group laughter.)

MS. HARRINGTON: We are wired up to many places, many people are watching, many people are listening who are not in this room, and there will be an opportunity for them to send in their questions.

I want to identify some of my colleagues who are around the room -- FTC staff -- they have little

green tags on the bottom of their name tags, and they're the ones who will have the microphones to take questions and involve you more in future panels.

And, before we break, I want to introduce three people who have really done this whole project. There are a lot of FTC staff people here who have pitched in and who are helping out with everything from, you know, making the coffee to arranging the chairs, we have people with Masters of Law Degrees who set up your chairs --

(Group laughter.)

MS. HARRINGTON: -- but there are three people who have really made this thing happen, and they are Brian Huseman, Renard Francois and Sheryl Novick.

(Applause.)

MS. HARRINGTON: Here's my colleague, Renard, who wants to say something.

MR. FRANCOIS: We have more time.

MS. HARRINGTON: We have more time? That's not what the agenda that I have says. Oh, great, what a bonus. Well, then, we can take questions. Does this mean that people won't get coffee, Renard?

MR. FRANCOIS: No.

MS. HARRINGTON: Wow! And they set up the chairs, they change the schedule, they make it all happen.

So, Brian and Sheryl -- and who else is there with a mic? Mona? Okay. My colleague, Mona Spivack.

Yes, sir. Right here -- Sheryl, give this gentleman right here in the blue shirt -- no, no, no -- behind you. Yes, indeed.

Your question? Identify yourself, please.

DAVID: I just wanted to ask -- Senator Burns mentioned -- internationally, if someone is in our rack sending out this Spam, how are we going to deal with that? We're talking more domestically, but, you know, will we prevent someone from going to another country? Does it comply with the U.S.? Does it want to comply with the U.S.?

MS. HARRINGTON: We have a whole panel coming up on that very subject and the question is, you know, what do we do about senders who are not within the United States, about the international dimension.

Chris, let me ask you your thoughts on that.

MS. GREGOIRE: Well, you know, I have to say to you that we're struggling even within the United States right now, and we do not have definitive court decisions now that allow us jurisdiction over, say, a sender from Florida, so we've tried to set up a partnership with the FTC, which is working most effectively, and with my colleague state AGs, where, for example, they've got a

sender in their state, I go to them, they try to take the action. If the sender is from my state, I try and take the action, which has been much more efficient and effective than me trying to take the action with a sender in Florida.

MS. HARRINGTON: Mona, could you give Commissioner Thompson a microphone, on the off-chance that he'd like to say something on that subject?

COMMISSIONER THOMPSON: Well, it just so happens that at the OECD we're working on this right now, working with 30 other countries to try to look at Spam issues. There's no easy answer here, but one of the things we're also working on is we're about to reach agreement on cooperation on cross-border fraud and deception, so that we can cooperate more freely, to address some of the problems that you -- the Attorney General -- just raised.

So, we're working on it. It's not easy, but there seems to be a growing consensus that this is a problem that needs to be addressed in a broader fashion.

MS. HARRINGTON: Okay. I see Brian has come into the room. Raise your hand. He's been working hard on this for months, and Sheryl. I just am going to introduce you at every opportunity, because this is such a phenomenal thing that you guys have done.

Next question? Where are my microphone people? Okay, Jason? Make it quick.

JASON CATLETT: I'd just like to get the panelists on the record on whether they think an anti-Spam law should be opt-in or opt-ed out?

MS. HARRINGTON: Okay, good question. Mark, opt-in or opt-out?

MR. FERGUSON: Confirmed opt-in -- there's a difference between opt-in and confirmed opt-in.

MS. HARRINGTON: Joe?

MR. BARRETT: Opt-in.

MS. HARRINGTON: Clifton?

MR. ROYSTON: Definitely, opt-in.

MS. HARRINGTON: Chris?

MS. GREGOIRE: Opt-in.

MS. HARRINGTON: Laura?

MS. ATKINS: Opt-in.

MS. HARRINGTON: Brian?

MR. ARBOGAST: Opt-in.

MS. HARRINGTON: Bob?

MR. WIENTZEN: Opt-out.

(Group laughter.)

MS. HARRINGTON: Thomas?

MR. COWLES: Opt-out.

MS. HARRINGTON: Okay, okay. Next question?

Sheryl, this gentleman right in front of you. We can't hear you and I need you to identify yourself -- just talk loud.

INAUDIBLE NAME/QUESTION.

MS. HARRINGTON: Did I need to repeat that?

GROUP: Yes.

MS. HARRINGTON: Okay. The answer is to the earlier question of how often are ISPs blocking IP addresses, and YAHOO is doing it once a second, every second, every second, tic-tic.

Okay, we have a question here in the front row.

TED GAVIN: My name is Ted Gavin from the SpamCon Foundation, and I'll sort of step off to the side for a moment. I had one question that was going to focus on free speech, but I think I'd like to ask another one, of Mr. Cowles, who earlier stated that his business was performing entirely opt-in but just advocated opt-out legislation, and I was wondering if he could speak as to how he reconciles those divergent positions.

MS. HARRINGTON: Okay, the question is to Mr. Cowles, you support opt-in in your business practices, but opt-out in legislation. How do you reconcile that difference?

MR. COWLES: Well, I don't think that other marketers or other companies should not have the

opportunity to have an initial conversation with the consumers. That's just my strong feeling. I think that Sears, JC Penney, should all have the opportunity to say, hello, I'm Sears, I'd like to do business with you.

MS. HARRINGTON: Okay. Do we have anything in the e-mail box that we want to get to? Who's got e-mails? Can you just run them up so I don't have to repeat them?

MS. SPIVACK: Yes. Understanding that direct marketers do not want to lose all rights to solicit new businesses via bulk e-mail, is it balanced to require that no more than three e-mails regarding one product or products from any one bona fide company be sent within a year period without a specific consumer opt-in to continue receiving such offers?

MS. HARRINGTON: Now there's a question. I can't possibly repeat that. Could you bring them up to me? And, Brian, is that what needs to happen? Do I need to repeat it?

Okay, here it is, again. Understanding that direct marketers do not want to lose all rights to solicit new business via bulk e-mail -- yes, we understand that -- is it balanced to require that no more than three e-mails regarding one product or products from any one bona fide company be sent within one year -- a

one-year period -- without a specific opt-in?

Okay, three bites at the apple, I guess is this question. Is it reasonable to give direct marketers three bites at the apple? Panelists?

Mark says, no. Joe says --

MR. BARRETT: Multiplied by every conceivable apple is a whole lot of bites.

MS. HARRINGTON: Bad idea, says Joe. Clifton?

MR. ROYSTON: I've seen estimates of around 27 million small businesses in the country, so 27 million times three e-mails you could be getting per year.

MS. HARRINGTON: Chris?

MS. GREGOIRE: How do you enforce that?

MS. HARRINGTON: Okay. Laura?

MS. ATKINS: It's a lot of bites of the apple, and there's going to be no apple left.

MS. HARRINGTON: Okay.

MR. ARBOGAST: It's a bad idea.

MS. HARRINGTON: Bob?

MR. WIENTZEN: Yeah, we don't think that's a good idea either. We think one bite of the apple ought to be it and that everybody ought to be aware of that and everybody ought to be able to be insured that that, indeed, is the case. So, that's why we suggest that opt-out be commonly known to be available -- available in all

e-mail -- and enforced when it is not effective.

MR. FERGUSON: Eileen, can I ask a question about that?

MS. HARRINGTON: Yes.

MR. FERGUSON: So, are you advocating that you're going to send Spam to somebody until they opt-out or send one Spam and if they don't reply, don't send them anymore?

MR. ROYSTON: No, we're suggesting that on every commercial e-mail there be an opportunity to say, I don't ever want to hear from you again about anything, and that that be respected.

MR. FERGUSON: But, if they don't respond, are you going to continue to Spam them?

MR. ROYSTON: Well, you're using the word Spam -- I'm going to continue to send them offers of $500 off on a new General Motors' car --

MR. FERGUSON: That's what junk e-mail is, Spam.

MR. ROYSTON: Well, that may be your definition, but it isn't necessarily mine.

MR. FERGUSON: It's actually the general definition accepted by the regular internet. MAPS has it on their website, mail-biz.org, as their -- they also have a mailing list standard that's been accepted for the

past six to seven years.

MS. HARRINGTON: The room is electric.

(Group laughter.)

MS. HARRINGTON: Okay, here's a question: If the DMA is truly in support of using existing laws to fight the Spam problem, why are they now also on public record as being against such actions; for instance, those underway in Utah? Who knew? What's going on in Utah, Bob, and what do you have to say about that?

MR. WIENTZEN: I don't know what's going on in Utah.

MS. HARRINGTON: Does anybody know what's going on in Utah? Emily, what's going on in Utah?

EMILY: There's a class action suit --

MS. HARRINGTON: Class action suit in Utah.

EMILY: -- where the local attorney has sent out probably 2,000 -- maybe 8,000 letters -- saying you are not in compliance with the labeling law in Utah, pay us $6,500 and we will go away. There's another law firm in Utah that's sending another --

MS. HARRINGTON: Okay, I get the picture. Class action law suits against Spammers, notices. We have a panel coming up on litigation issues, later in the forum, and that's one of the issues that we'll be talking about.

Question in the audience, over here. Sheryl, right there. I can't hear you. Question from overseas. She's from France.

MARIE GEORGES: I was surprised that probably the last question that was raised -- I was surprised when hearing about unfair practice and so forth. Nobody really talked about fair collecting e-mailer question. Why is it not a problem for you? You talk about unsolicited e-mail, but in this big problem, there is a collection of e-mail. Why don't you talk about the question of how to collect e-mail in a fair way.

MS. HARRINGTON: How to collect e-mail addresses in a fair way?

MARIE GEORGES: In a fair way.

MS. HARRINGTON: Okay, so the question from our friend from France is why aren't we discussing the legal fairness involved in practices used to collect e-mail addresses? And, what do you know, we must have paid her, because that's what the next panel is about, which is going to led by my colleague, Eric Wenger. So, Eric must have paid her to ask that question. Good job, Eric.

MR. ARBOGAST: Can I answer that question?

MS. HARRINGTON: Yes, Brian.

MR. ARBOGAST: I think that any concept of kind of best practices in commercial e-mail sending has to

address how you get the e-mail names in the first place. So, that's key.

MR. ROYSTON: And the whole issue of harvesting, I think, is a very important one that we need to come to a definitive answer on, and we believe that the surreptitious collecting of e-mail addresses, no matter how you cut it, is just not an acceptable practice.

MS. HARRINGTON: Okay, we only have time for a couple more questions. In the back row, there.

MR. MCGUIRE: David McGuire from washingtonpost.com. What do you think of a Do Not Spam Registry like the Do Not Call Registry?

MS. HARRINGTON: Senator Schumer is going to drop in this afternoon after he drops in his bill, I think that would create that, and we have a legislation panel coming up on the last day, and I think we'll get to that then. Okay? We want to keep you here for three days.

We have a question over here.

(Inaudible speaker identification/question.)

MS. HARRINGTON: How do we address the mailer issues, both in practices and legislation. Laura, that's your client's case, so what do you have to say on that?

MS. ATKINS: I think in terms of the mailers,

that the senders and the people that actually pay you guys to send them out, are mostly responsible, but the mailer industry, itself, has the responsibility to police their customer base. And if you have customers that bring you a dirty list, then you need to hammer on them and make them stop, and it's your responsibility to make sure that your customer base is clean and that they're not causing you to send Spam on their behalf.

MS. HARRINGTON: You need to be certain that you've got a good list of people who opted-in rather than harvestees.

Mark?

MR. FERGUSON: You could require confirmations for each e-mail address.

MS. HARRINGTON: Confirmation for each e-mail address.

MR. FERGUSON: And what that means is you can get the confirmation replies. If somebody approaches you to do a mailing -- Brian, I think DCentral is in that business -- basically, what you can do when they bring you a list is ask for confirmation for each e-mail address on that list. And if they don't provide them, then more than likely it's a dirty list. If there's no confirmation for them.

MS. HARRINGTON: All right. None of this,

obviously, is scripted, but for a completely spontaneous moment we have just a few seconds. Commissioner Swindle, would you like to say anything at the end of this panel?

No? A completely spontaneous "no" from Commissioner Swindle.

All right. Well, we have come, I think, unless Renard tells me that we've just readjusted the schedule again, that's it. Okay, this is the end of this panel. We will take a 15-minute break -- no more. We will be right on time for this program.

(Applause.)

(Whereupon, there was a 15-minute break from 10:15 a.m. until 10:30 a.m.)

MR. WENGER: Okay, we have a couple of housekeeping matters to get started here. This panel is going to run from now until about 12:05, and then that's when we'll break for lunch. So, we're about 10 minutes different from the original printed agenda.

We need to make sure that everybody on the panel here speaks into the microphone. When we have questions, we're going to have to repeat them, because the folks on the phone and on the video-conference can't hear what's being said on the roving microphones.

And, the other housekeeping matter is I want everybody to know that there are garbage cans out in the

back there. Apparently some people think that this is like a movie theater and you can leave the popcorn under the chairs, and we don't have anybody to come and clean all that up. We have people who set up the chairs, but please take your trash back out.

Okay, so, the timing for this panel is going to work like this: I have a couple of demonstrations up front and then we're going to save some questions at the end, and I have about seven or eight minutes for each panelist to talk about the topics that are assigned to them. We have a pretty tight time schedule, because there's going to be another event in this room at 12:30 and, then, we have to pick up here again at 1:30, and we're going to start sharply at 1:30. So, I can't really go over on this panel.

Okay. We have a very distinguished panel here, and I'm just going to run down who's on here, very quickly, before I dive into it.

We have Rob Courtney, he's a Policy Analyst for the Center for Democracy and Technology. Rob is right here next to me.

We have Matthew Steele is at the head of the table there, and Matthew is the Senior Director for System's Engineering for Brightmail, Incorporated.

Then we have Doug McLean, who's the Vice

President for Corporate Marketing for Postini, Incorporated.

And, then, directly to my left is Richard Smith from computerbytesman.com, a noted security expert.

Next to Richard is Gil Terriberry, who's from Direct Contact Marketing Group.

And, then, is David desJardins, Software Engineer from Google.

And, then, finally, William Waggoner from AAW Marketing.

We're going to start off with a quick presentation from Matthew Steele from Brightmail and Matthew is going to show us some techniques that could be used to verify e-mail addresses and also to harvest them from websites.

So, with that, Matthew, if you're ready, I'll ask you to dive right in.

MR. STEELE: I'm ready as soon as I get the screen. All right, here we go.

So, I'm going to talk briefly about e-mail harvesting/e-mail verifying and show you a quick demo of that, and the tools we use to do it. So, really quick, before I kick off the demo -- actually, I'll kick it off in the background while I'm talking.

So, what's going on here is we've got a couple

of addresses: One for Brightmail and one for the FTC, and this tool is reaching out, hitting those domains and peeling through those domains looking for e-mail addresses, collecting anything it can find on the web.

One of the first, actually tools, people used to get started with this is just search engines, not that search engines are Spamming tools, any way, shape or form, but it's a place where people go out to find addresses for top areas where they want to start collecting addresses.

And, then, once they've done that, so, let's just say I happen to have a garage full of spurs and --

(Group laughter.)

MR. STEELE: -- and I needed to find somebody who wanted to buy those, I might go out and search, using a search engine, like under spurs, with topic areas, and you'll find discussions, groups and website. I mean, I guarantee you there's a discussion group out there that's all about spurs.

And once you found that spur website, you take a tool like this and point it at the website and it'll go through and just collect every single e-mail address it can find on that site.

Now, this tool is not only looking at the actual address that it's touching, but it's following the

links from that address over to other websites and collecting addresses from there.

MR. WENGER: And is it looking through the HTML for an "at sign -- @" or something, or --

MR. STEELE: Yeah, there's different tools, but it's basically going through looking for mail-to links or actual just e-mail addresses. So, it'll look for anything connected to either side of it, and then collect all those into a list.

Depending on the site you're hitting, how fast your connection is -- I think during a test last night I was collecting about 200 mails every two minutes -- about 100 mails a minute for this particular tool. So, you can get a pretty good collection of lists.

So, again, they'll find a topic area, take a tool like this, and you just can start collecting addresses.

MR. WENGER: And how expensive is something like this?

MR. STEELE: Well, this particular one, you can get for about $40. So, these tools range from, you know, free scripts that people have written or for something like this -- this is probably at the low end, but it's still pretty powerful -- for about $40 up to about $200.

MR. WENGER: And you're an engineer, but would

I have to be an engineer to run something like this?

MR. STEELE: No, it's pretty much like you can go in there, type in your e-mail or address, the same way you would for a browser, hit go and it goes off and collects e-mail addresses for you. So, they're very, very simple to use.

Now, once the tool is done, and I'll just show you, you just actually click -- you can see off to the right in the panel, the actual web addresses it's hitting. And, then, over on the other side, this is all the e-mail addresses that it's collected.

And, so far, in the course of me talking, we've gone through 138 pages on Brightmail's website and collected 27 e-mail addresses.

So, once these addresses are collected, what you end up with is a list. So, the same thing -- point and click, you hit one button on this tool, and it saves your list off into an XML file -- or, sorry, this is an Excel file.

MR. WENGER: I see people that I know, actually, on this.

(Group laughter.)

MR. STEELE: Yeah, so, as the FTC was participating in the conference, I did do a brief collection of addresses off of your website.

So, again, this is a collection I pulled off the FTC site, actually, last night before I came in here.

So, once again, you put it in your URL, you hit a button, it generates a bunch of addresses, you hit another button and now you have this really nice list in Excel, it's all been very difficult so far.

So, the next thing that needs to happen is these addresses need to be verified, so being the kind people that they are, they provide you a tool for that, also.

So, now what this is going to do is basically I'm going to browse to the file that I just built, tell it where that file is, it's going to start collecting those addresses and now we're going out and actually verifying those addresses to see if they're real.

So, obviously, not every link or e-mail address on a website is real.

MR. WENGER: And how does this verification work?

MR. STEELE: Well, essentially, what's happening is whenever you send a piece of mail, the first thing that happens at the destination address is the mail comes in and there's a little sort of handshake that goes on to establish whether or not the person you are sending to is really there. And that all occurs before any

content even is gone to the location where you're sending the piece of mail to the individual.

So, what this tool does is it goes through and just does that initial conversation, checks to see if this is a real address; if someone is really there, and then, if it is, it then cleans the list and then saves it off into another file for you.

MR. WENGER: So, it's going to the port for the mailserver, giving the name that it wants to check as if it was going to send an e-mail message?

MR. STEELE: Yeah.

MR. WENGER: And, then, noting whether or not it gets a valid or invalid response for that e-mail address and just terminating the process of sending the e-mail message at that point?

MR. STEELE: Let me show you that, actually, precisely. So, here's just a single -- this is the tool doing it just like one single address. So, I put in one address, mine, and this has reached out -- for those of you working with e-mail systems, this is very familiar, and for the rest of you, this is probably kind of Greek -- but what it's done is it's done the first part of that conversation of check. It does a little hello, like, hi, I'm there --

MR. WENGER: Like a handshake between two

people.

MR. STEELE: -- like a handshake, like, hi, I'm somebody, and that somebody has used some bogus address. And, then, it says, this is who I want to send some mail to and it checks to see -- and let me actually jump right over to there and -- all right, so right here, where you see at the very bottom of that, you see it's validated against Brightmail server and it says, "connection closed." It reached out, said hello, said, I want to send an e-mail to this person. The system said, great, this person is there, and then it just exited and left.

So, from the end-user perspective, from you folks out there receiving mail, you're never going to actually see that this even occurred.

MR. WENGER: But the mail servers are seeing repeated requests to send e-mail messages that don't end up in generating e-mail messages?

MR. STEELE: They are. So, there are -- and actually I think that's probably addressed in another panel -- so in the interest of time I won't get into techniques for stopping that.

But, what we just went through in about five minutes was we've harvested a couple hundred mails and then we verified those 200 mails and peeled it down to a list of valid addresses. I think at the end of that I

came up with about 150 valid addresses that I could then start sending mail to.

So, that kind of walks you through, briefly, about how someone who wanted to create their own list would generate that list and start sending mail.

MR. WENGER: I should say this was not intended to be like a "how-to," we're just trying to show how easy it is --

(Group laughter.)

MR. STEELE: Yeah, I thought about that yesterday -- like, how do I make this so you guys can't go out there and do this? But, it's relatively simple these days, and one of the aspects of Spamming with regards to tools, and it does touch on this panel, it's not just one of the ways folks are making money or commercial enterprising here, is selling lists they've created, verifying lists, and selling tools to allow folks who have large garages full of spurs to go sell those spurs on the internet.

So, in addition to this, aside from just using the tool to collect addresses, people also get CDs and stuff. They'll take a CD of addresses and use the verification tools and actually go verify those addresses and stuff.

The other thing that's not really shown here,

once you've actually gone out, collected some addresses from a site -- especially if it's somebody targeting commercial entity -- they can sort of identify a naming convention. You know, it's like, you know, bob.smith@somecompany.com.

And, then, there's another set of tools you can use, once you know the naming convention, to then use that to randomly generate more addresses, based on the naming convention, so that you can send more mail.

MR. WENGER: Okay, great. Thank you.

MR. STEELE: Thanks.

MR. WENGER: We're going to turn next to David, and he's going to tell us a little bit about the experience of Google and what's happening there and what they're seeing about e-mail addresses are gathered.

MR. desJARDINS: Great, thanks for inviting us to participate. I want to talk about --

MR. WENGER: Could you just hold up your pen for a second?

MR. desJARDINS: (Complies.)

MR. WENGER: I don't know if you can see, but it's just turning a lot of different colors.

MR. desJARDINS: It flows in the official Google colors, I think. And we have a few of these as door prizes.

So, I just wanted to start with a brief observation, which was, you can search on Google Groups, which is an archive of the past 20 years of discussions, and you'll see for Spam you'll find that the first real discussion of commercial Spam was in April of 1994. So, it's interesting that a problem that has this scope is less than 10 years old.

Google is really focused on helping people find information they need, and, hopefully, to improve the experience of using the internet. And, on our own side, we go to great lengths to ensure that our interface is clean and simple and easy to use and to show people relevant information.

That's led to Google being very popular. Unfortunately, people do sometimes use Google to find things that aren't really what we would want them to be finding. And we definitely do see people using automated tools or software to search Google for pages or sites that contain e-mail addresses. And, it's logical to infer that they're doing this in order to collect e-mail addresses for Spamming purposes.

This takes place at difference levels. The simplest thing might be just somebody who's searching for a site for discussion of spurs and, then, they're going to run one of these harvesting programs on that. At

Google we wouldn't even know that that's what they're doing; they're just looking for spurs and you can't tell the difference between somebody who is looking for a site about spurs to discuss the spurs or a site for spurs to harvest the e-mail addresses. And we wouldn't see, then, the harvesting, because that's done with a separate program that doesn't go through Google.

We do, also, see, though, people sending very large numbers of searches to Google where they're searching much more extensively over the whole web for pages that are likely to contain e-mail addresses or for sources of e-mail addresses.

And people who send automated queries to Google in large numbers like that violate our terms of service and it's a problem for us and we take whatever feasible steps we can to prevent that.

But it's not practical to block all such queries. And, particularly since Google's goal is to help people find stuff, we tend to err on the side of allowing any kind of information retrieval and preventing people from using the service is, really, only a last resort.

So, these automated queries can, sometimes, cost Google a significant amount of money, impose a load on our service, degrade the quality of service for our

users, but we're still very cautious in doing anything about that.

Whenever people are collecting e-mail addresses, directly or indirectly, through Google, all the information that's in the Google web index is publicly available in other ways on the web. The Google Web Search is just compiled from websites that are open to anybody with an internet connection or a web-browser. And, so, it's possible for individuals or organizations that want to collect data, it's possible for them to use Google. But it's also possible for them to just go directly to those websites.

MR. WENGER: And the same holds true for the groups, as well, is that you're providing the interface for looking at these groups?

MR. desJARDINS: Yeah, I was going to get to groups separately, but that's true with groups, too. The groups data that we have, the messages that are posted to Google Groups -- Google Groups is one view of Usenet, which is a worldwide discussion service -- and all of the messages that are on Google Groups are also -- if it's posted on Google Groups, it's sent by us to other Usenet servers all around the world. And, you know, frankly a Spammer could set up their own Usenet server and join Usenet and get every Usenet message and filter them, and

that's inherent in the way the service is constructed.

So, any messages that people see on Google Groups, that do have e-mail addresses in them, people might -- and sometimes they do -- harvest -- because Google Groups is one of the biggest interfaces to Usenet -- people do harvest e-mail addresses from Google Groups and we certainly block that when we can. But, at the same time, even if we able to completely prevent that, it wouldn't really solve the problem because those messages are out there lots of others places.

We know from the CDT study that Usenet postings, in particular, are very aggressively harvested for e-mail addresses. And I don't think that all of that -- or even most of that -- is through Google.

Going back to the web, it's possible -- it's really not that hard, with even relatively modest resources -- and this is sort of what Matt was showing -- for people with relatively modest resources to go out and harvest directly from websites; particularly if they have some idea of what they're looking for -- targeting some area -- and what to call certain sites, and harvest e-mail addresses from them.

And it's also more effective, in some cases, for unscrupulous people to go directly to the websites because they can defeat or bypass mechanisms that Google

respects, whereby the webmaster can communicate what information they want, accessed or not accessed.

So, there can be sites which have indications on them, like robots.txt files that indicate that the webmaster is saying, we don't want search engines or automated processes to visit these pages -- that might be conceivably something you might put on some sort of discussion group in an effort to avoid collection. And Google would respect those because our policy is, very strongly, we're only trying to index and search information that the owners of that information want us to index and search.

But somebody who is running one of these tools, I would guess, there's a very high probability that they're doing it anonymously and they're going to, in fact, duck and run if they got detected anyway, and they aren't particularly interested in observing any rules that the webmaster might put forth.

So, in that sense, Google isn't the most effective to get at the information on some sites; going there directly is, actually, going to be more effective.

So, just to sum up, search engines are a big way that people find information on the web, and e-mail addresses are no exception. But, really, I think, search engines are a relatively small part of the problem, and

even if there were no search engines, people would still be able to find the e-mail addresses that are out there.

MR. WENGER: Okay. Thank you very much. And you filled almost to the minute, or to the second, for the amount of time that I allotted you, you filled. So, that was perfect.

I think that when we told Senator Burns to come here and to make some comments that might spur the debate, he maybe took that too literally.

(Group laughter.)

MR. WENGER: That example seems to be the one that's going to prevade the whole day.

I'm actually going to go now -- because David actually mentioned the CDT survey and, then, he also mentioned how harvesters deal with robots and things like that, we're going to Rob from CDT next, who's going to actually talk about his survey, and then Richard Smith will talk about some of the things that he's done to see how you can, maybe, foil the harvesters. And, so, let's turn to Rob now.

MR. COURTNEY: Thanks very much. CDT undertook, in the late part of 2002 and the first month of 2003, a six-month's study to try to evaluate how Spam is sent, and particularly how Spam addresses get picked up by people who send Spam and the various ways that a

user might, intentionally or otherwise, reveal or disclose his or her e-mail address and whether certain kinds of activities might lead to more Spam and other activities.

We posted about 250 different addresses on different parts of the web, that included public postings on websites, as was referenced, it included postings on Usenet. It also included disclosure to a number of popular web services and companies and things like that to evaluate when a user discloses his or her e-mail address and makes various selections on the kinds of interaction they want to have with those services, whether that can lead to unsolicited commercial e-mail.

I do want to take a second and say that the definitions we use when we talk about Spam are very important. I think, frequently, you may find that no two people use the same definition. I want to be clear that the definition we used was unsolicited commercial e-mail in cases where there had been an opt-out or we had maybe opted-in to mail and then asked not to receive it, we counted as unsolicited anything that came within two weeks after our attempt to opt-out. And this is all available in the methodology on our website, which is www.cdt.org.

Just to deal with the part of our study that

specifically referenced the topic of this panel, which is harvesting, I think it will not be surprising to anyone that the overwhelming majority -- somewhere over 98 percent -- of all the Spam we received was to the six addresses that were posted on the public web.

We received about 8,600/8,700 e-mails over the entire project; about 8,500 of those were to addresses that had been posted on public websites. And, so, clearly there is an issue here.

We only posted on a relatively small number of websites, but there seems to be an initial correlation between the popularity, the number of hits a website gets in a given period of time and how much unsolicited e-mail we received at those addresses posted on those websites.

We did, also, post on Usenet, we posted in, I would say about, maybe, 15 different Usenet groups, and we received about 150 unsolicited e-mail messages to those addresses.

I do want to take a second and talk about that we did not only test putting addresses on the web or putting addresses somewhere to see what would come back. We also tried to test some popular methods that you sometimes see people use to try to avoid getting Spam. And that includes things like writing out their e-mail address in English as opposed to in plain text machine

language, writing, "this is rob@cdt.org" and I might write, Rob, R-O-B, at, A-T, C-D-T. D-O-T, O-R-G.

We use that, and in cases where we obscured the message in that way, we did not receive a single unsolicited commercial e-mail. So, all 8,500 of the e-mails we received to publicly posted addresses were to addresses that were posted in the standard form.

We tested another thing, which for some users may be a little bit arcane, but for people who are familiar with HTML will sound maybe familiar, we tried encoding e-mail addresses using the HTML special character codes, and those are things like and sign (&); number sign (#), 087 semi-colon (;), and there's one of these codes for each letter in the ASCII set.

We encoded the addresses in that way, and the interesting thing about doing that is when you use HTML special characters, when a web-browser retrieves the page, it has a built-in parcer and it understands those and immediately translates it into usable text.

What we were testing was to see whether a Spam harvesting program would do the same thing. Our results indicate that they do not. We did not receive a single e-mail to any of the addresses that were encoded in that way.

MR. WENGER: But your intention is that if you

post your e-mail address you're trying to put it in a way that a person could see the address and understand it, but you want to try to fool the machine. And, then, I guess if you're doing it in a way that's easy enough for a person to figure out what it is, then the people who are harvesting can adjust what they're doing.

MR. COURTNEY: And that's exactly the point I was about to get to, that many people have e-mailed us to say, well, you're just giving short-term medicine, the Spammers will adjust and they will build their tools to do this. And that may happen -- that may also happen for this Rob-at-CDT-org. That's a very simple transformation. Time will tell on that.

I would flag one thing which is that anyone who took the time to obscure their e-mail address is probably not a person likely to respond to an unsolicited offer of commercial services. And, so, for anyone who may be in the audience or in cyberspace thinking of redesigning their tool, maybe it's not worth the time. And I certainly hope that they will take that approach.

(Group laughter.)

MR. WENGER: And, I guess, if you look at it from the analogy that was used by Senator Wyden about the burglar rattling all the doors, that you first try the ones that are unlocked.

MR. COURTNEY: Exactly.

MR. WENGER: And it's easier to get the addresses that are written out in the standard @.com format.

MR. COURTNEY: Right. But, I mean, I want to say that it is a legitimate thing to say that this may change over time and this approach may be less effective.

I do want to address one other thing, which I know we'll spend a little time talking about in this panel, which are these so-called brute force and dictionary attacks on mail servers. I know this is not strictly harvesting, per se, but I want to bring it up because I think the ISP operators in the room will probably nod their heads and say that these are a serious problem.

We set up a very small, it turned out, box to handle this project, and about halfway through the project it was bombarded with thousands and thousands of -- it actually was a brute force attack where they would try to send an e-mail to every single possible combination of letters on the server.

So, it would start with A@the address; and B and then AA, AB, AC. We got about 8,600 of those e-mails before we frantically pulled the plug, because our system was choking.

And, so, I do want to say that is a problem; the ISP operators we've spoken with have said that it is a problem. The nice thing is, once the attack is happening, you can block the address if you catch it in time. The downside is if someone has a short e-mail address, like rob@cdt.org, you may get a lot of these before your operator is able to pull the plug.

And I'm running out of time, but I do want to say, unfortunately, CDT has very boring pens, and no door prizes -- what I do have is copies of the report. So, I hope that anyone who doesn't get a pen you can come get a copy of the report. It is also available on our website.

And the very last thing I will say, we have had several requests from people saying, can I see the data? You have these 8,600 e-mail addresses --

(Group laughter.)

MR. COURTNEY: -- well, not addresses, but e-mail messages. The messages are defunct now, there's no point in Spamming to them. And we will be doing that. Anyone who wants to see it -- several hundred megabytes of messages -- should come and talk to me. We're distributing it on CD because our bandwidth operator had no interest in serving up that much data. But we do have it and we have a list of each address and what it was used for.

Thanks very much.

MR. WENGER: Okay, great. I'm torn now, because we also have Doug, who can talk about the dictionary attacks that were just mentioned, but I'm going to stick with my stated plan, which is to go to Richard next and talk about some of the techniques that you can use to deal with harvesters on your website.

MR. SMITH: First of all, I want to say thanks to CDT for running this study. It was a real eye-opener when I saw it last month, and it got me thinking about, well, are there countermeasures possible? And Rob's already mentioned one here of using HTML and coding. But I think there's some other possibilities that are out there.

And, doing a little bit of research with Google, it looks like not a lot of these areas have been explored, and I think one of the messages we're getting out of this study, as well as some other things I'm going to talk about today, is that harvesting is really the air supply for the Spam system.

So, I want to ask the question is it possible to cut off that air supply? I don't want to suggest this is a universal solution to the Spam problem, but it may be one area that hasn't been explored too much.

To give you an idea, I would recommend for

everyone to go home to run a little experiment, which is simply to go to Google and type in your e-mail address and find out how many web pages you show up on. I did that a couple of weeks ago and it's like 1,200. And, so, I get a lot of Spam.

But whenever somebody says to me, why am I getting so much Spam? I tell them to run this experiment. I think it's extremely important.

Now, on the issue here, there are sort of two sides to this -- looking at the harvester issue. One is hiding e-mail addresses so that humans still can use them but that a harvester can't. And Rob's mentioned the HTML and coding, a URL coding, and I think that's a good method and I think it clearly will work today. I tried out six harvesters and none of them understood this HTML and coding. So, it's a good way to go.

But, we're in an arms race here and once the software vendors are aware that their products are not being effective, they'll go switch over. But, then, their customers are going to take awhile to update it. So, I think this could -- one small thing could last, you know, a number of years.

Another approach that I've seen a little bit and then I've invested more carefully is using scripting code to generate the e-mail addresses on web pages. And,

by doing this, you actually raise the cost to a harvester, because it would also have to execute the code in order to find the e-mail addresses. And I think that may set a high enough bar that it would go a long way of cutting off e-mail addresses to the harvesting companies.

MR. WENGER: Now, what you're suggesting here is that the HTML code would not have a mail-to tag that's written -- you know, it wouldn't say, you know, your exact e-mail address, it would have some JavaScript that would generate the information on the fly, so that when you load the web page, the web browser would interpret the JavaScript and then display the e-mail address, but if you looked at the source code it would not be obvious what e-mail address is going to be there. And, then, if you wanted to have a harvesting program that was going to pull that address out, it would have to execute the JavaScript and slow it down?

MR. SMITH: Right, that's the idea. And there's two places e-mail addresses kind of occur in web pages; one is in the text, that you can see it; and, then, the other place is in the mail-to link. So, you want to have JavaScript code handle both of those cases.

I looked at even going one step further and saying, well, what if they execute a JavaScript code, well, what else can you do? Well, the next level up in

the arms race is to have the mail-to links generated when the user clicks on them as opposed to when the page is loaded. And I think that will set a very high bar for these guys.

So, I think this is an area that should be looked at. As I said, in my Google searching it didn't seem like a lot of attention has been paid to this area.

Now, another part of this harvesting thing is to try to identify harvesters at the time they're doing their dirty business and then taking counter measures. And, you know, I think at Google they're already doing some of this, but I think that the websites could do this, also.

And I just ran an experiment with some of these programs -- the atomic one was one of the ones I tried out. And they're very easy to fool, which is what you do is you put them in the spider trap so they get hung up loading pretty much the same page over and over again, not getting e-mail addresses.

My website can be spidered in about a minute from a DSL connection and by putting in a loop, these programs ran for hours. And, so, if we did a lot of these, again, we could raise that economic cost. But, again, it becomes an arms race.

So, the way this might be able to work out is

that we have companies that provide the spider trap service to other websites.

On the issue of hiding the e-mail addresses, one thing that I wanted to highlight, is I don't expect people -- regular folks who are building websites -- that go off and, you know, hand-code all these addresses. I think the right approach would be the tools that are used to generate web pages automatically do this for people.

And, so, one of the things that I want to get out -- sort of the word out on here -- is that, you know, the people who make FrontPage or contribute from MacroMedia, should look at this as a new feature in generating web pages.

I don't see this as a universal solution. You've got millions of millions of people literally generating web pages, but if we can get the tools that create web pages to do this, I think we'll help out this problem.

Thank you.

MR. WENGER: Okay, great, thank you. You're up, Doug. We're going to talk now about the dictionary attacks, and these are the software code programs that will attempt to generate e-mail addresses through sort of a brute force attack.

MR. MCLEAN: I'm Doug McLean, I'm the Vice

President of Marketing at Postini, and I want to spend just a minute explaining who Postini is, because I'm about to show you some data and some graphs that are really pretty incredible in terms of the amount of directory harvesting that is going on, and without some understanding of where we collect this data, there may be some credibility issues.

We're the largest e-mail security services provider in the nation. We've been around about four years. We currently have about 1,000 customers who range from very, very small ISPs with 50 users to the very largest industrial and service companies and law firms and investment banks in America.

About four million end-users use us every day to block both Spam and viruses from their networks and their personal computers. On an average day, now, we process about 75 million pieces of mail a day. We believe that makes us the fifth largest e-mail processor in the world.

We sit at what's called the SMTP layer, and for those of you who aren't e-mail engineers, SMTP is the protocol that the net uses to pass e-mail around. And we instrument that layer to watch for Spam attacks, virus attacks and what we call directory harvest attacks, and we see these things occurring in realtime, 24 hours a

day, seven days a week, aimed at our users.

There's been a lot of discussion already this morning about how much Spam there is in the network. Before I got down into exactly how much directory harvesting attacking is going, I thought you might like to see what we saw last year, just in terms of Spam fraction on the net.

As we came out of Q1 last year, it looked to us like the amount of Spam on the net was actually leveling off at about 25 percent; certainly annoying but manageable.

What happened in Q2, there was a significant jump in mail, a little bit of leveling in the summer lull, and, then, as we headed into Q4 and the Christmas buying season, we just saw this relentless month-by-month increase in the fraction of junk e-mail aimed at our four million users. And what we have today, at the end of Q1, is that in a basic day about 75 percent of the mail that is attempted to send to our users is junk -- unless you think that we have users that are just particularly bad consumers of Spam.

I attended a panel just a week ago today down in Baltimore at ISPcon and there were representatives of both MSN and AOL on that panel, and the AOL showed a graph of the amount of attempted deliveries, which is

actual deliveries on the AOL system, and guess what? It's also about 75 percent junk.

So, it is our belief that overall, in the wild, on the net at the moment, about three-quarters of the e-mail in transit is Spam. Is the legitimate e-mail infra-structure we all depend upon every day under siege? You bet it is.

The other thing we see, very quickly, is the standard deviation around that average is really broad. A lot of our customers only get 20 percent Spam, even today; 80 percent and 90 percent is, unfortunately, not at all uncommon.

I'm actually going to skip over this and talk to you about what these brute force attacks look like. The demo that Matthew did, in our view, is actually the behavior of a relatively good actor in this drama. And the reason is that they at least have the courtesy to go out and try to find good addresses on a news group or a website first before they, then, attack the mail server to verify it. Because a lot of Spammers, I will tell you, don't bother anymore.

What they do is they start off with these lists of 100,000 text strings, in front of the @ sign; they aim them at a domain's mail server or servers, in very, very high volumes, and they just keep asking over and over

again -- is Bill there? Is Steve there? Is Gates there? Is Smith there? And every e-mail server on earth is hard-coded to answer that question honestly. In fact, it's even worse for somebody calling Exchange 55, which is the version that Microsoft is trying to get everybody to upgrade from at the moment, doesn't answer that question in a very timely fashion; it actually tends to wait awhile. And Spammers tend to interpret that as a good address. And, then, turn right around and Spam it. And, so the Exchange 55 service, at least that we protect, tend to get, percentagewise, more Spam than the more modern ones that return invalid address responses faster to the Spammers.

So, what eventually happens is, they hit a good one; they immediately open an SMTP session and send a piece of Spam. Or, they may just wait until it collected 15 or 20,000 addresses and do that all at once a little bit later.

We have domains on our system that are literally under brute force attack, 24 hours a day, seven days a week. It tends to be the better known consumer brands that have very large and desirable employee basis standing behind them that the Spammers want to get to.

The way our service works, very briefly, is we have a connection manager on the service that blocks

these directory harvest attacks. It only takes us about 12 invalid calls to identify that and block it. We have a number of technical techniques for doing that and during the Q&A maybe we can dive into that.

We map these things every single day on our website. I'm afraid this map probably doesn't resolve very well for a lot of you, but the red and the purple dots that you see on this map are the directory harvest attack sources that we saw one day back in January. There were only 40 millions messages that day for us, it wasn't a huge day, but we saw 20 million pieces of Spam.

We also list everyday on our website the top 10 harvest attacking IP addresses, just because we think it's good to illuminate them. And what we tend to see is that very soon after a directory harvest attack from a source address, the Spammer turns right around and starts sending Spam. We actually had a day last week -- and there's always huge correlation between where the harvest attack comes from and where the Spam comes from. We had a day last week where the top three addresses on our attack map and our Spam map were identical.

And, just for a little bit of context, we also publish everyday a similar map on where viruses come from. It's all a domestic affair, for the most part. You tend to infect your friends.

Harvest attacks and Spam, at least aimed at our users, more than 50 percent of it already comes from overseas. Huge amounts from Pacific Rim; South Korea is day in/day out, you know, the number one or the number two source; a fair amount from Japan; Singapore; Brazil is an immense source of Spam at the moment.

MR. WENGER: But, Doug, you can't tell whether or not the person who is launching the attack is actually, let's say in Brazil, where that IP address is located or if they're just coming over the internet and then going through an open relay, right?

MR. SMITH: We know, for a fact, that particularly the things we see coming in from the Pacific Rim are open relays that domestic Spammers are paying to have held open for them.

And, to wrap up very, very quickly, this stuff happens just in incredible volumes. Hundred thousand so-called directory harvest attacks followed by 25,000 Spam attacks on a domain over the course of an hour. It happened everyday on our service. It's just an immense problem.

And, the final thought I want to throw out on this, is that legislation is a good idea, but given the amount of this stuff we're seeing coming in from overseas, particularly from countries where the U.S. has

never had any luck coordinating intellectual property law, it's going to require a global effort. Our rule of thumb at Postini is, if you can buy Windows XP or Office XP for $10 on a street corner, you are probably standing in a jurisdiction that is developing and broadcasting a huge amount of Spam.

And that's me, thank you.

MR. WENGER: Okay. And Matthew has a couple of seconds to add about the way that they deal with these issues at Brightmail, as well.

MR. STEELE: Just touching on different technologies and approaches, we work a lot with what we call ProbeNetwork, so we'll see a lot of the packets coming in, we can recognize the dictionary attacks as they come in through the network. And, then, we'll generate filters to go out and catch that stuff at sites where we have our software deployed, which right now represents about, I think, 50 billion messages a month we're filtering through different agencies where we have the stuff deployed.

And, in that context, because in some instances you have situations where you have sort of a relay in front of the system that moves through it like, as Doug was talking about, the Exchange 55 stuff, and you want to try and catch it a little bit ahead of time or you have a

situation where the address, with brute force attacks in particular, they're not even necessarily paying attention and validating them, they're just sort of sending.

So, we work with identifying that stuff up front and trying to block it before it can actually get back into the place where it gets validated, to try to save that sort of strain on the systems.

There's a lot of different approaches, technically, to dealing with this stuff and there's a lot of, I think, evolution we all have to do in the industry in terms of trying to keep up with this.

MR. WENGER: Okay, great. Before we turn away from the technology portion of this panel, I wanted to invite our panelists, if they have anything they want to contribute as we're going along, just to take your table tent and turn it up on its side.

MR. WAGGONER: I want to add something.

MR. WENGER: Okay, go ahead, sure.

MR. WAGGONER: To Brightmail and about this dictionary attack question we're talking about here, it's Brightmail's policy that -- I watched you guy's convention you guys had just recently on the americanspamconference.org, I think it was, okay?

MR. STEELE: Yeah.

MR. WAGGONER: And dictionary attacks, I mean,

you have to number one determine, you know, what is a dictionary attack and what if somebody is sending a real list and cleaning their list? I mean, just because somebody is sending or validating their list, so to speak, does not mean they're attacking your servers.

So, I hear all these different statements about filtering and this and that and everything else, I mean, but Brightmail, you guys do recommend that people that do e-mail marketing clean their list. Is that correct?

MR. STEELE: Yeah, we do.

MR. WAGGONER: Okay. So, I just wanted to make that clear that not everybody that's sending a list out there and doing the verifying situation is doing a dictionary attack. Do you agree there?

MR. STEELE: Yeah, I mean, it's an excellent point. It's just that the tool I showed you guys earlier to verify addresses, I mean, and I think, you now, to Doug's point, it's sort of like being a good actor, that can be used as a valid tool to check and validate that addresses are real without having to do a dictionary attack. And tools like that are used by valid bulk mailers.

MR. WAGGONER: Thanks.

MR. MCLEAN: We actually ask our customers to configure what tolerance for connection attempts their

system will sustain, because a number of them agree with your search and a number of them don't care that you're cleaning a list and just don't want to deal with the connection attempts.

MR. WAGGONER: You know, another thing, too, you guys might want to think about is that the problem here with Spam and people that -- you know, when I hear the word Spam all the time, I think of evil people, you know, trying to scam you, okay? Spam and e-mail marketing are completely different things. I mean, people that I consider Spammers are people that do not care what they send or who they send it to or they do not honor your opt-out policies or, you know, I'm in the marketing business myself and I post on the Google news groups and a lot of the anti-Spammers sign me up for lots of different newsletters. So, this is on my AOL account, believe it or not, and I get about 60 to 100 every single day due to the fact that the anti-Spammers, people trying to fight this so-called fight, now they punish me with this.

So, anyway, I tried the same exact thing you have done with trying to opt-out of these so-called legit newsletters and it doesn't happen -- you know, it doesn't happen at all, you know. It's interesting.

MR. WENGER: An interesting point has been

raised. When you talked before about the process of checking e-mail addresses and you said that was at least someone who was going through the process of doing some verification. So, I mean, does everybody agree that at least it might be a better practice, from the standpoint of the mail servers, to have the e-mail addresses verified before somebody just starts sending messages indiscriminately?

MR. STEELE: Well, yeah. I mean, there's no reason to send a piece of e-mail to an address that doesn't exist. So, there's no reason for these brute force attacks.

MR. WENGER: But there's still a drain on the resources of the servers in the process of verifying, as well, right?

MR. STEELE: Well, sure, verifying, too. I mean, obviously it would be -- if you're going to have commercial mailers out there, it would be nice if they had valid, previously established relationships with the people they're going to send mail to, because even verifying is going to put a load on the server.

MR. COURTNEY: I would just also say that, I mean, I think -- I have a couple of points. First of all is that -- and we have been naive, but our methodology in our study was that our mail server was set to accept

pretty much anything that came in because we had so many e-mail addresses that were being sent and we parced it after the fact. Now, I guess, in this case, we paid the penalty for that -- we ended up with almost 9,000 messages coming in because the mail server did not reject them as invalid addresses, it sort of accepted anything that would come by into the system.

The second part I would say is that, you know, validating an address in this method -- I'm not a technologist, so I won't comment on it's merits -- but I will say it's not the same as, you know, we talked about opt-in and opt-out and people sometimes use the term validating in a different context, which is the context of confirming a relationship or having an opt-in relationship.

MR. WENGER: That's a good point. We're not talking here -- here we're talking about the techniques of grabbing e-mail addresses and checking whether or not the addresses exist, so that if you sent them e-mail, we're totally removed now from the issue of whether or not somebody wanted to receive whatever e-mail would result from that.

MR. WAGGONER: Can I say one more thing here -- I've got --

MR. WENGER: Actually, I've going to turn to

conversation to you and I'll give you an opportunity to talk about how, in your business, you get the e-mail addresses that you send the commercial e-mail messages to, if you wouldn't mind.

MR. WAGGONER: Okay. I'm been in the e-mail marketing business about seven years. I originally got into the business the way a lot of what everybody's talking about here with the different little softwares and things that you can buy, you know, it's all over the internet. And for somebody that's my age and an entrepreneurial type thing, you know, you're looking at ways to make money on the internet and it's the new way out there -- it's the new economy, it's the new way of doing things.

So, seven years ago I got into the business and it's been great, but as I progressed through my experiences in the business, you know, obviously I had to learn the hard way about the way things are on the internet. There's a lot of internet etiquette, so to speak, you have to do. I mean, you don't want to Spam people, like exactly what we're talking about this whole time here. I mean, I know people do not want to get Spammed; I don't want to get Spammed; I get it every day.

So, anyway, I have, over the years, bought my e-mail addresses, I have different websites -- thousands

of websites all over the internet --

MR. WENGER: Can I just ask one question -- are you sending messages on behalf of products that you're selling or do you have clients that you're sending messages on behalf of?

MR. WAGGONER: We have companies that hire us to do marketing for them --

MR. WENGER: Okay.

MR. WAGGONER: -- and that's how we do our --

MR. WENGER: And do they supply you -- let's say I have a product I want to sell and I come to you, do I supply you the list of e-mail addresses I want you to send it to?

MR. WAGGONER: Typically, no.

MR. WENGER: No.

MR. WAGGONER: We have our own lists, specifically, you know, different categories of people of different types of products, you know, that kind of thing -- demographics. But we get them from all over the United States. You know, from people I've sent for free offers, for free Playstation 2s, we do giveaways, you know, we do vacation packages, things like that. Business opportunity leads, mortgage leads, you know, auto insurance, life insurance -- things like that. And we, you know, categorize it out like that and that's how

we develop our list, generally over the --

MR. WENGER: So, are you saying you use different lists for different types of products?

MR. WAGGONER: Yes, exactly.

MR. WENGER: Okay. So, first let me ask you two questions: How do you get the e-mail addresses that you're going to send to and, then, how do you decide which of your lists you're going to use?

MR. WAGGONER: Okay, well, I mean, it just depends. If someone goes through one of our websites, we'll pop-up, we'll pop-up, or something like that, and you'll see a little e-mail address box with, you know, different categories to check, you know, what you're interested in and things like that, and you submit, boom, it comes to us, we send a confirmation out to them, and they confirm and click on the link, that's when they get their e-mail. That's how it works with us.

MR. WENGER: These are websites that you operate that people are visiting?

MR. WAGGONER: Yes, we buy traffic from other websites all over.

MR. WENGER: The world?

MR. WAGGONER: Yeah.

MR. WENGER: So, in other words, somebody might have a link on their website that would feed to you?

MR. WAGGONER: Well, no. Like Google has banner Traffic you can buy, you know, AOL -- everybody has banner ads you can buy. They supply pop-unders or, you know, different software that you can buy from download.com that, you know, and it gives you little pop-ups.

MR. WENGER: Would your websites be advertising a product or they're advertising the ability to receive e-mail from you?

MR. WAGGONER: Yeah, the ability to receive e-mail, of course. It's like, you know, there's different offers we offer people. You know, like a free vacation package and they sign up and we'll send them the information on how to do that, you know, or send the leads to a lead broker that is looking for a, you know, individuals looking for, you know, free vacations or mortgage ads. I'm sure you've seen that out there before.

MR. WENGER: So, if you know that you're going to be doing ads on behalf of a mortgage broker, you might have a site that asks people if they're interested in receiving leads or something --

MR. WAGGONER: Right. After we have got the lists, over periods of time, then we would go ahead and someone would hire us to send out their offer for

mortgage leads or whatever the product might be.

So, let's say, for example, we have a website or there's a website that's putting a pop-under for, say, a vacation, if a vacation company wants to hire us to generate traffic for them later to develop leads, we would do that for them that way.

MR. WENGER: Okay.

MR. WAGGONER: Does that make sense?

MR. WENGER: Yes. David is itching to respond to the mention of Google.

MR. desJARDINS: Yeah. I just want to point out that Google does not, in fact, have banner ads or pop-up ads, and we have a pretty strong position against that and a problem with that. There's actually a problem -- and I'm sure I haven't seen any of William's sites, so I don't know, specifically, but we have a problem, in general, with pop-ups which can, within themselves, be deceptive in the sense of you're not sure when you see a window who it's associated with, and that there may be legitimate uses for pop-ups, but there's a lot of deceptive pop-up and pop-under advertising or software that generates windows where somebody may be entering information into a window because they've been misled into thinking it's associated with one service or site and it's actually something else.

MR. WENGER: So, if I go to Google and I see a pop-up window or a banner ad, it means that there might be something on my computer that puts that there?

MR. desJARDINS: That's definitely true, and that's why another kind of problem is software that may be installed on your computer without your knowledge. Google's been pretty aggressively trying to fight this because people do, sometimes, get things installed on their computer where they aren't quite aware of what they're getting, and then there may be pop-ups. That may be generating windows or requests for information that they are mistakenly thinking are associated with Google.

There's also the problem of people mistyping addresses that they're going to. Some people may mistype Google and go to something that's spelled something like Google --

MR. WENGER: Like Gogle --

MR. desJARDINS: -- that may redirect them to Google but also generate a pop-up window with some other kind of advertising. So, there's a lot of confusion -- I don't want to say deception, because you can't always infer people's intent, but there's a lot of confusion on the web and people may be -- it does relate to, you know, address gathering, I think, because some of these sites or softwares will, then, generate requests for

information and people may think that they're providing information to one service, when they're really providing it to something else. This is sort of one of the many reasons why confirming is really important.

MR. WENGER: Do you have any thoughts about some of the technological means that we were talking about before?

MR. WAGGONER: Yes, I do. Let me address what he just said about Google not promoting pop-ups or pop-unders, you know. Overture and Google, you guys are tied together, right?

MR. desJARDINS: No, that's not right.

MR. WAGGONER: In no way, shape or form?

MR. desJARDINS: No.

MR. WAGGONER: You guys don't accept money in any way at all for traffic, huh?

MR. desJARDINS: That's correct.

MR. WAGGONER: Okay. I can see that you believe that, but the thing is that there's ways to get e-mail addresses, okay? People buy traffic to get people that want their e-mail. So, that's how we do things. We don't deceptively lure people to our websites or have any pop-unders that fill out forms for people or stuff like that.

I mean, if you can show me a website that

actually you'll fill out a form for me, you know, man, that would be amazing -- I've never seen that happen. So --

MR. WENGER: I think the suggestion was that a form might appear on a website and you might not realize that it's not associated with the website because there's some JavaScript or something.

MR. WAGGONER: Well, it wouldn't happen with JavaScript. You're talking about, like, spyware programs?

MR. WENGER: Yes, exactly, like a window and you might fill out the form. I don't think we're suggesting that the form would be completed automatically.

MR. WAGGONER: It just sounded that way. But, yeah, there is, you know, spyware programs and you download some kind of little, whatever little thing off of download.com or whatever, and installs a bunch of different little spy worlds and it would hit you with different ads. That's annoying, I agree.

MR. WENGER: Do you want to comment about whether or not you agree with the use of programs that will gather e-mail addresses off of websites?

MR. WAGGONER: You know, I don't see anything wrong with it. I don't think it's a smart way to do

things. I think that people who are going to spam the way that we're talking about here as a problem are going to get e-mail addresses no matter where they come from. They'll buy CDs; they will steal them from anyplace they possibly can get them, okay?

So, what I wanted to address as well is back to the verifying situation about the way filters are set up to prevent people from getting e-mail addresses off of servers. You know, I don't really think the problem is getting the e-mail addresses. I think the problem is -- for example, Spammers that are unethical people that are trying to just -- don't care about practices and just looking to make money. Companies like America Online, for example, you cannot validate your e-mail addresses with them. You could send a million e-mail addresses to America Online and America Online will therefore turn back and say that every one of them are good. Now, what I think, I mean, I think -- sorry.

MR. WENGER: We'll have AOL people on later panels that can --

MR. WAGGONER: I mean, that's the thing, I mean, AOL literally sets people up for their statistics. This billion -- I block a billion spams a day, I mean, come on, let's get for real. I mean, that's the complete biggest fraud I've ever heard in my life. Okay, that's

just -- it's garbage.

MR. WENGER: Two billion they said.

MR. WAGGONER: Two billion spams a day, yeah, okay. Maybe they're counting in the situation where -- because if you do -- I mean, all these Unix boxes and Microsoft servers or whatever, typically, like we said, it's a universal thing where they have it built in so you can validate an e-mail address, say, is joe@aol.com there? You know, Spammers, you know, guys that really don't care about the rules are going to sit there and just bombard servers all day long. They don't care who's there or not. So, our point is that --

MR. WENGER: Do you want to draw a line for me about where you think the difference is between yourself and people that you say don't care about the rules? In other words, what do you think those rules are or ought to be that ought to be respected?

MR. WAGGONER: Number one is that the rules are that if you're a legitimate marketer and you have legitimate contact information, for example, how you guys found me. I mean, you guys looked me up and there I am. I mean, William Waggoner, there, I'm in the phone book in Las Vegas, Nevada. I'm not hiding from anybody.

Now, Spammers are people that are going to hide from people. They're going to use fake e-mail addresses

as from addresses. They're going to use bogus URLs in their actual ad itself, things like that, you know, people that are actually, you know, those chain letters, you know, those types of things. That's what I consider spam.

MR. WENGER: Could we now try to distinguish where you think the rules are or ought to be about -- if any -- about the source of e-mail addresses that should go into commercial e-mails.

MR. WAGGONER: Say it -- repeat that for me.

MR. WENGER: Do you think there are or ought to be any rules about where you would gather e-mail addresses for sending commercial messages?

MR. WAGGONER: Personally, no. No, I don't think there should be any rules. I think that as long as people are held accountable for their actions after the opt-out request or --

MR. WENGER: And I don't mean law. I mean, I'm asking about, you know, sort of --

MR. WAGGONER: Rules as far as like the community of internet that --

MR. WENGER: Netiquette kind of rules, right.

MR. WAGGONER: Not necessarily, no. I think that if you post your e-mail address on the internet, you are going to open yourself up for someone who's going to

e-mail you, offering you some kind of ad. I don't care what kind of program, what kind of filter you put up, it's just going to happen. I mean, it's a public deal all over the world, and people are going to find a way to do this.

I think the solution to this whole problem is simply everybody, not only Spammers or bulk e-mailers or whatever, it's the AOLs, it's the Yahoos, it's the Hotmails, it's the Brightmail. It's everybody that have a set of rules that they follow that make it -- because the thing is is that what happens here is that legitimate e-mail marketers are hurt by Spammers. That's what is happening on a daily basis.

I mean, I can get my e-mail addresses all day long from people actually going to my websites that are listed in google, okay? And sign up for my mortgage list or whatever they want to sign up for, but if Brightmail filters me, or if AOL filters me, based -- because they have these new programs they're building to fight spam, who's it hurting? It's hurting legit market like myself. And what's it doing? It's -- yeah, who's laughing? It's funny, huh? Try and make fun of those things? Yeah, real funny. Yeah, you probably work for Bright -- They're good guys. I like you guys.

MR. STEELE: Yeah, I do work for Brightmail

actually.

MR. WAGGONER: I know. Well, you know, other guys make livings off spam-fighting. It's both sides of the fence. But I'm saying Spammers aren't -- it doesn't matter what filters Brightmail puts together, AOL, it doesn't matter.

MR. WENGER: Before I turn to our last panelist, I just want to ask you one more last pointed question, from the last panel about whether or not you agree with -- where you fall on the opt-in, opt-out. And if you're sending a message out to one of your lists, do you believe, and I'm going to stick to sort of a netiquette rule, that there ought to be an opt-in on that list? In other words, you shouldn't be on that list unless somebody has confirmed with you that you want to be on that list?

MR. WAGGONER: I believe yes, people should opt-in, some kind, absolutely.

MR. WENGER: Okay, and that if you do send a message to people you believe that there ought to be some way to get off that list?

MR. WAGGONER: Absolutely, with my stuff personally, I mean, we have about five different ways to opt out of our list just right there in the e-mail message itself. I mean, they can actually go to the

website there, there's different links to do, but you know, there's a myth out there. What's that?

MR. WENGER: No, I was just motioning to Gil that he's next.

MR. WAGGONER: There's a myth out there by anti-Spammers out there that if you click on an opt-out link or if you send your e-mail to somebody to be removed or call an 800 number to be removed, don't do that, they're going to send you spam, they're going to send you more spam. You know, maybe that's true with some people, but not everybody. I mean, you know, for example, my company, if somebody clicks on a link to be removed off all our lists, I mean, it's an immediate situation. You don't have to wait. It's done, done deal.

So, I think, you know, we're talking about making programs to -- for, you know, web harvesting, you know, to prevent people from obscuring their e-mail address or whatever on their website. I mean, that's impossible to do. Average Joe people that want to build a website and put it on the internet, they're not going to, you know --

MR. WENGER: Right, although Richard's point with regard to that was that the automated tools for generating websites on geocities and things like that --

MR. WAGGONER: Oh.

MR. WENGER: -- ought to have -- for instance, when you want to type -- I want to put an e-mail address on my website, it would take whatever steps are necessary to do.

MR. WAGGONER: That's a good idea. That's a great idea. I didn't actually hear the word geocities and free websites mentioned.

MR. WENGER: I didn't -- I just used that as an example.

MR. WAGGONER: That would be a good idea, yes.

MR. WENGER: Okay, Gil, let's turn to you now and let's talk a little bit about your business, tell me a little bit about who -- where you fit into the scheme of things, who the parties are when you're doing your business and the mechanics of how messages get sent. And you gave me an example actually when we talked on the phone about a wine list, maybe you want to give that as --

MR. TERRIBERRY: Well, it is a good example. First, okay, I'm also an e-mail broker. I'm a list broker, in fact, postal and e-mails, I'm responsible for the stuff you got in your regular mailbox, too.

MR. WENGER: You are trying to win friends here?

(Laughter).

MR. TERRIBERRY: And influence people. What's -- Bill's right. Spam has poisoned the well. Successful e-mail marketing is harder and harder and harder because response rates are down because people are ignoring all commercial e-mail. Now, there are some, I think, right ways to gather addresses. I'm not talking about the technology, I'm talking about the philosophy of gathering an address.

MR. WENGER: Before we get to the right ways to gather e-mail addresses, just tell me about why, in your opinion, e-mail is an important tool. You talked about it as a leveling device.

MR. TERRIBERRY: Well, the internet's -- we're really talking about a completely different paradigm. We're also talking about a place where half of the people who go on the net haven't been there for three years and don't understand how to obscure an e-mail address to begin with. It's the first time we've set up a marketing mechanism where there is a mechanism for marketing where the folks being marketed to can shoot back.

And that changes things entirely. It's not television; it's not print advertising; it's not push advertising; because the folks that are receiving the e-mail have ways to literally shoot back. I mean, you --

MR. WENGER: Not in this room.

MR. TERRIBERRY: With postal mail, we used to have a joke about okay, tape the reply card to a brick so they have to pay more in postage when they get it back. With e-mail --

MR. WENGER: Does that work?

(Laughter).

MR. TERRIBERRY: I'm not going to answer that. But with e-mail, you can use mechanisms like "Spamcop" to report the mailer and actually get his internet connection closed down, sometimes, depending upon who he's connected with and how bulletproof his server is. There are things that the consumer can do with regard to e-mail that can't be done, even with telephone marketing. I mean, Telezappers frankly don't work.

The folks that I work with, the folks that I -- my clients are mailers who are going to targeted lists, both postal and e-mail. My vendors are list owners who have permission to send third-party mail and who get paid to deliver a certain -- to a certain specification a message that's being sent by a client. There are really four elements in there. One is the permission. Now, I don't care whether it's opt-in or opt-out or check the box or uncheck the box or whatever. But if the person who is being added to the list understands what they've given permission for, however it's done, that's step one.

The second step is identification. If I subscribe to a publication, I have a business relationship with that publication. I've given them permission to send me marketing messages that I consider relevant. When the e-mail comes to me, I should be able to recognize that it's coming from the New York Times or Time Magazine or Computer Week, and not someone I never heard of.

Relevancy, the message does need to be relevant to the interests that I expressed and the ability to unsubscribe immediately has to be there. You put all of those together and it's not a spam problem, and you don't need a filter, because the people receiving the mail know who it's coming from, know they have a relationship, know they gave permission and know they can make it stop.

MR. WENGER: So, let's say I sign up for a magazine or some website and they ask me if I want to receive additional information and they give me a list of categories and I check off that I want to receive things about.

MR. TERRIBERRY: Mm-hmm.

MR. WENGER: I supply an e-mail address; I say it's okay to send me things. That company is what you're referring to, I think you said as a vendor.

MR. TERRIBERRY: They're a vendor.

MR. WENGER: Okay, so they --

MR. TERRIBERRY: They own that e-mail list.

MR. WENGER: -- own the list, and they're going to send out the messages on behalf of the client.

MR. TERRIBERRY: I come to them with a client that wants to reach parents who have purchased educational software for their kids.

MR. WENGER: Mm-hmm.

MR. TERRIBERRY: Or who have expressed an interest in educational software. We contract with the list owner to send that message under the list owner's name. To that specification, and the response is obviously go back to the entity that's actually doing the marketing or is actually selling the educational software. But it's a relevant message.

MR. WENGER: And you're reminding them essentially that through the use of the name that this is where you went originally and you expressed --

MR. TERRIBERRY: You signed up at, you know, ivillage and said you're interested in this stuff and here we're sending it to you, we're not endorsing the offer obviously.

MR. WENGER: Right.

MR. TERRIBERRY: And, by the way, if you don't want us to do this anymore, we'll stop; all you have to

do is reply to the e-mail.

MR. WENGER: So, the advertiser who -- on behalf of whom the message is being sent never actually sees the list.

MR. TERRIBERRY: Never actually sees -- the advertiser -- we talk about renting lists. We don't really rent lists. We contract for a service. We contract to deliver a message to a designated specification or designated audience. Now, the other end of the spectrum, we've got the one I told you about, the small wine store. He's here in Herndon, he's got subscribers to his newsletter all over the country, because it's a neat newsletter with some good wine information --

MR. WENGER: But he started in print, right?

MR. TERRIBERRY: -- and some good recipes. He started in print. It was costing him $1,200 to $1,800 a month to mail just to folks in Fairfax and Loudon County.

MR. WENGER: And how does that compare to what he's doing now?

MR. TERRIBERRY: It doesn't cost him anything. I mean -- any people want to receive the message and he can promote or he can talk about a specific product and see it in his store the next week selling. What that does, the lack of expense in sending e-mail for the small

business has leveled the playing field. He can go out and compete effectively with Total Beverages, and there's no way he's got their marketing budget. That's the wonderful democracy that's occurred with the internet and e-mail.

MR. WENGER: I'll get to you in a second, Richard, but can you tell me how that model, how it should work, is affected by the untargeted sending of spam that the same people who are on that list are receiving?

MR. TERRIBERRY: It costs us money. And Bill made the point that now that the well has been poisoned, response rates, even to solicited requested permission e-mail are going down to the point where they're starting to look like postal mail. You know, worst than that, the quality of the responses are not as good as postal mail was producing to begin with.

And if I'm giving a company advice, I'm telling them to go back to the post office right now.

MR. WENGER: Do your clients -- or the vendors that are sending on behalf of the clients run into problems with having their messages blocked by filtering or black lists --

MR. TERRIBERRY: Very seldom. Very seldom. If they were not following their own protocols for --

MR. WENGER: But even assuming that they're following --

MR. TERRIBERRY: -- gaining permission that -- there would be unsubscribes and typically on any contracted send, you're going to lose about 20 percent to hard and soft bounces and nondeliveries.

MR. WENGER: Right.

MR. TERRIBERRY: Some are going to be out of office, some are going to be bad addresses.

MR. WENGER: So, the point that you were making, and I sort of stepped on what you were saying was that you have the reason for keeping the list clean and following your permission rules --

MR. TERRIBERRY: Absolutely.

MR. WENGER: -- because otherwise the list becomes less valuable. But the point I was -- the question I was trying to ask was even if you follow your own rules, because the well has been poisoned and because there's so much stuff that's going on that's filtering and blacklisting, does that make it difficult for people who are even trying to send to specific permission-based lists to get things through?

MR. TERRIBERRY: In 1997, I did an e-mail for a trade show, an IT trade show, using Network World Fusion's e-mail list. It was a brand new list. We only

found 7,000 addresses on that list that were IT managers who had an interest in or buying authority to buy document management, imaging management software. The e-mail went out and my client's server was buried by people coming in to register for the show floor pass to come to the trade show. That doesn't happen anymore. It just doesn't happen.

MR. WENGER: But is that because --

MR. TERRIBERRY: Because folks don't own the -- they don't open their mail because it's embedded in 60 other pieces.

MR. WENGER: -- they're not opening messages or because they're not -- right. Or is it because the messages are not getting through? Is it a combination of --

MR. TERRIBERRY: From where I'm sitting it's because of signal to noise. It's the noise of the spam that's clouding or blocking the signal that would be what we'd call the legitimate e-mail.

MR. WENGER: They get so much stuff in their mailbox it's hard for them to recognize the things that they asked for.

MR. TERRIBERRY: I filter mine into several different mailboxes, including one bulk box.

MR. WENGER: Right.

MR. TERRIBERRY: I have a business, so things come into that box that are from addresses that I've never seen before that my God, they may be customers.

MR. WENGER: Right.

MR. TERRIBERRY: So, I have to look at that bulk box, but yeah, I get tired and I check the box that checks all of them and just blow the whole box away from time to time.

MR. WENGER: Right.

MR. TERRIBERRY: That's not a good thing.

MR. WENGER: Bill, did you have a comment about that?

MR. WAGGONER: Yes, as far as like as it filters and too much spam, I think it's both. It's definitely both. Because a lot of things, I mean, you don't really know if your e-mail's getting through some of the time, like it was talked about before, because of like, you know, the way AOL will just let anything through. You know, America Online --

MR. TERRIBERRY: I'm my own ISP. I know what's getting through.

MR. WAGGONER: Well, I wouldn't say that, I mean, unless you know -- I mean, I got that work for me real high-tech guys and, you know, I'm very meticulous and know for a fact that my mail's getting through and

there's ways you do it, but the only -- I mean, you don't know 100 percent. These filters out there, there's a lot of ways they block a lot of things. So many filters out there, I mean, you really just don't know.

MR. WENGER: Okay, we have about 15 or 20 minutes left, and let me just see if there's anybody else on the panel who wants to comment about anything else that we've talked about before we turn to the audience here.

Richard, did you have something?

MR. SMITH: I just have a real quick thing here.

MR. WENGER: Okay.

MR. SMITH: You know, on this issue of sort of demarkation of marketing and allowing the little guy to help out, you know, I saw a few heads shake in the audience how it's a good thing. But what we're really dealing with here is of course the classic, you know, tragedy of the common issue, and it is so cheap to send stuff out, and we're just getting in a feedback loop where we have to send out more and more stuff we feel like to get our message through. And I don't disagree. I think, you know, something like targeted newsletters that you sign up I think are a great thing. I'm on a bunch of them myself, you know, and I love that kind of

stuff to get news. But unfortunately, you know, we do have to deal with this cost question, you know, when it's so cheap or almost nothing to send out e-mail, we're in a sort of a negative feedback loop of just going to get ever increasing at this unless we do something about it.

MR. WAGGONER: Who's calling anything cheap? I don't -- I always hear this whole myth about e-mail -- sending e-mail is cheap. If you guys knew what my internet bill was on a daily -- I mean on a monthly basis, it would floor most people in this room. So, I mean, I don't know what cheap we're talking about.

MR. WENGER: The question is how much?

MR. WAGGONER: More than probably you -- a lot, thousands, okay, there we go.

MR. WENGER: Okay. Gil, sorry, go ahead.

MR. WAGGONER: Thousands, there we go.

MR. WENGER: You need to speak into the microphone, though, Gil.

MR. TERRIBERRY: Yeah, back to --

(Laughter).

MR. TERRIBERRY: Okay, fine, back to Richard's point about how to -- it's so cheap. Asking the technologists in the room, somebody here, can you tell me how to make it cost to send bulk e-mail and still have it free for me to send e-mail to my mother?

MR. WENGER: I think we'll save that for future panels, to talk about the fixes later on, yeah. We're going to -- it's a thought-provoking idea, but --

MR. TERRIBERRY: Well, you need to be able to tell the --

MR. WENGER: Right.

MR. TERRIBERRY: -- and what do you make it cost for this little wine store --

MR. WENGER: Right.

MR. TERRIBERRY: -- who's not Chubb Insurance.

MR. WENGER: Right. Let's take some questions from the audience here, because we have 15 minutes about to go. There's one right over here. Go ahead.

MR. GOLD: Hi, Jacob Gold. I was just curious, we're talking a lot about spam, direct marketing, are we distinguishing between newsletters, people -- I get like newsletters, people want to express their ideas, as opposed to selling a product? Are we focused on both or is this just about people selling products? Because I haven't heard much about newsletters at all, which are more annoying.

MR. WENGER: I think the focus of the panels in this workshop is on commercial messages.

UNIDENTIFIED SPEAKER: Which may be embedded in the newsletters.

MR. WENGER: Right, and newsletters can serve a dual purpose. In other words, the wine newsletter may give information about wines, and the reason you sign up for it is because you want to learn more about wines. At the same time, he has a business of selling wines and he's -- so he's hoping that he's going to cultivate business by sending you information.

MR. COURTNEY: I would just add that I think he's highlighting -- we're having highlighted here an important point, which is that the line between commercial and expressive is not always a very bright one. And when we talk about defining spam, whether it's on a panel like this or whether it's in legislation, it's important to be very careful so that you don't accidentally make your net too small or make your net too wide, and you catch things in the net that maybe you didn't want to.

MR. SMITH: I would just say that unsolicited newsletters are spam. You know, if -- particularly like you get in the investment area. Those aren't really newsletters, you know, even though they call themselves that. So, I think that's just another way to mask, you know, another sort of semi-deceptive way of dealing with things.

MR. WENGER: The question that preceded that,

I'm sorry, was about are we talking about newsletters here or advertisements. I should have repeated the question.

Yes, over next to Stephen here.

MR. BEAR: Hi, this is Josh Bear (phonetic) from Skylist. One thing that I just repeatedly came to mind as this conversation has gone on that I think is important to point out is just that harvesting is one big part of the problem, but I heard somebody mention on the panel that if that were to go away there'd be no source of addresses for the spam problem to exist, and I really think that's totally not true.

There's one other huge side to it, which is a coregistration business model that's built around offering free services and sites, as I think -- I think as Bill was referring to -- specifically for the purpose of generating people to give their permission so that you can then mail to them. And there is a huge business around that that I think we'll probably see at the economies -- economics of scam -- of spam talk -- same thing -- that, you know, that I think is a really big piece of this problem, too, and I just wanted to point that out and see if you guys agree with that.

And a side point I wanted to make is I have a telezapper and it really works.

MR. TERRIBERRY: Actually, the technology --

MR. WENGER: Can you repeat what he was talking about first and then address it if you had a comment on it?

MR. TERRIBERRY: Okay, what was he talking about?

MR. WENGER: The question was about dual registration models, is that correct?

MR. BEAR: Just that part of the problem is harvesting. That's definitely -- that's half the problem.

MR. WENGER: Right, and that's what this panel's about, right.

MR. BEAR: That people generate these registrations for the purpose of getting their permission. They get permission when they do it, but a lot of people right now think that's spam when it goes out, and so it comes -- you get to the definition thing --

MR. WENGER: So, the question is that somebody might sign up for something but not recognize it when they get it as being something that they agreed to possibly have received?

MR. BEAR: It's not really that clear, but yeah, that's --

MR. TERRIBERRY: Well, also if it becomes totally irrelevant, it's perceived as spam.

MR. WENGER: Right. One of the -- when you laid out your business model, you explained that part of it -- it has to be that the message is relevant to what you signed up for. In other words, I said I'm interested in, you know, model airplanes or something.

MR. TERRIBERRY: Then don't sent me a Penthouse offer.

MR. WENGER: Right. So, if the message is too far off from what I agreed to, then even if I gave permission, people might perceive it as being spam if we're assuming that spam is what people perceive it to be.

MR. TERRIBERRY: The other thing, Wientzen was asked in the last panel, or asked where we would get addresses to send marketing e-mail to, sort of on the presumption that ISPs are common carriers and like the post office they've got to deliver his messages. There are a million ways to collect those addresses from print advertising, television advertising, your web presence, if folks want to get information from you, they'll find you. There are enough advertising venues that are push advertising that you don't have to co-opt e-mail as a push venue.

MR. WENGER: Okay. Richard, did you have something?

MR. SMITH: Yeah, I want to address that issue. I've done some experiments with that, a little bit, but not a lot. There was a website called web million, millionweb, something like this, a bunch of executives just went to jail for stock fraud, but anyway, that was a different issue, but, you know, they were a sweepstakes site, you know, that's a classic example of just collecting, you know, blind e-mail addresses. And I still get stuff from that.

I ran this experiment a couple of years ago. My feeling -- but I'd love to see a study of this, and maybe that's in the next generation study for CDT -- my feeling is, though, that represents a relatively small percentage of the spam that's out there, and I agree it is spam. Now, the problem that I have with it is it's sort of this gray area. When you do the opt-out, you're opting out with somebody who bought the e-mail address and not the source, and there seems to be no way to go back to who's really giving this away.

MR. WENGER: Jeff Fox from Consumers Union?

MR. FOX: Just want to ask Rich and Rob about this idea of cutting off the air supply for harvesting. I was very happy reading the CDT study to see that when

you pulled an address off of the website the spam went down. But then it was kind of an in vitro study; that's not -- you know, you put -- the address -- up and then you took it down and that was the end of that, you know.

As Rich points out, you know, when you do a search on your e-mail address, and I've done some google searches, there's a letter I sent to a federal agency, not the FTC, in July of 1995 that's still up on the web. There's a posting to a listserve who never told me they posted to the web. And I can find dozens of references there, even if I, you know, want to take my e-mail address off of my own page, it's not using, you know, HTML and path-dot techniques. There seems to be, short of changing my e-mail address, no way to ever remove those references.

MR. WENGER: Okay, the -- Jeff was referring to Richard's comment earlier about how that if you look at harvesting as being a part of the problem that if you were able to somehow deal with the harvesting you might be able to cut off the air supply for where the spam is coming from. And Jeff was pointing out that a lot of times the e-mail -- the websites that have the e-mail addresses don't just come down the way that they did in the CDT study.

Right, and he gave an example of having filed a

comment with a different federal agency that has his e-mail address on there and it's still there; or there may be archives of old web pages and it's just very difficult to undo something once you put it out there on the internet. I think that's a very interesting point.

Mona, you have an e-mail?

You want to give it to me, because that way I don't have to repeat it?

MS. SPIVACK: Yeah.

MR. COURTNEY: While it comes, I have a quick response to what Jeff was saying.

MR. WENGER: Yes. And then I saw a hand waving over here, and we'll get to you next.

MR. COURTNEY: And I think the quick response to what Jeff is saying is that he's absolutely right, that this is a problem, that an e-mail address is a valuable thing and once it's out, even if you take it down from one site, if it's on 10,000 sites on google, you know, and you can see it through google how many sites it's on, it's out there. And I think there is part of an education thing which can happen here.

I think many -- you know, there's a need for consumers to sort of be aware of that when they give their address out, that once it's out, it's out, and there are tools out there that can help users with this.

And I think a lot of people in this room probably operate multiple e-mail addresses. I myself have an e-mail address that I, you know, I will disclose to people I do business with or I'll have an e-mail that I use for public postings, and I have an e-mail address I use for my family.

And that's a small step. It's not a silver bullet, but it's something that people can do to try and assert a little bit more control over this problem that once they're out, they're out.

MR. WENGER: Your study addressed both of these issues. You had services that you signed up for and then tried to unsubscribe from.

MR. COURTNEY: Right.

MR. WENGER: And, so, that deals with where you're voluntarily providing it for what you think is a specific purpose.

MR. COURTNEY: Right.

MR. WENGER: And you want to be able to revoke that permission. The other part of the study was where you just put out an e-mail address for general contact purposes and you were looking to see whether or not that address was going to be picked up and used for commercial purposes, right?

MR. COURTNEY: That's right.

MR. WENGER: Okay. I have a question here from the e-mail. It says I have a question for Mr. Waggoner or Mr. Terriberry. Could they please tell us the exact address, and you can choose not to answer this, of their websites where I can opt out of their e-mail lists. Thank you.

MR. TERRIBERRY: Too many to list.

MR. WAGGONER: I don't have any e-mail lists.

MR. WENGER: Because the vendors operate the e-mail lists --

MR. WAGGONER: Right.

MR. WENGER: -- and you're basically forming connections between the vendors and the advertisers?

MR. WAGGONER: Right.

MR. TERRIBERRY: However, if they want to go to my website, it's dcmg.com, and they can find out how I do business.

MR. WENGER: They can find information there about how you do business, that's correct. Okay. Mona, you had a question?

MS. SPIVACK: I do. I have my own question for Mr. Waggoner and Mr. Terriberry. Do you as a broker and as a sender of bulk e-mail do any quality control to see that your client's e-mail message, the underlying content of the e-mail message, matches up in any way, shape or

form with the subject line or the from line of the e-mail?

So, for instance, if you have somebody who's selling adult content internet messages, the underlying message has a pop-up with adult content. Do you do any quality control to make sure that the subject line is not misleading or deceptive in any way to sort of dupe somebody into unwittingly opening adult e-mail?

MR. WAGGONER: We never --

MR. WENGER: Before you answer, let me just quickly repeat, because there are people who can't hear. The question was whether or not there's any quality control done. I'll ask the specific question about whether or not there's an effort to make sure that the subject line matches the content, in particularly in regard to adult entertainment.

And then I'll also append to that a question about whether or not you seed, for instance, seed the lists in a way that you can see what's being sent and just checking up on the mailings generally.

MR. WAGGONER: Well, the last part of your question, yes, there are ways to tell, you know, who's opening what and how much response it's getting, things like that. But no, we never, ever use deceptive practices to get somebody to open up an e-mail. Like

there's a lot of subjects you see like hey, I saw you in a chat room, or hey, how are you, or hey, we got a meeting tomorrow, stuff like that, and then you open it up and it's, you know, whatever, some kind of pornographic ad or whatever. We absolutely do not do that whatsoever. What you read in the subject line is what you get in the e-mail on the website itself.

MS. SPIVACK: So, do you affirmatively check then?

MR. WENGER: He's sending the messages, right, in his model, he's sending the messages, so he would -- I'm assuming --

MS. SPIVACK: No, no, you have clients that hire you to send e-mail --

MR. WAGGONER: Oh, absolutely, absolutely, absolutely. We never -- we don't -- we don't send out an e-mail for -- with a subject line about mortgages and then they get to the website and it's porn. No, absolutely not. Is that what you're asking?

MS. SPIVACK: Yeah, whether you affirmatively take steps --

MR. WAGGONER: Absolutely, 100 percent, 100 percent.

MR. WENGER: Now, Gil, in your model, you're not actually sending the messages.

MR. TERRIBERRY: No.

MR. WENGER: So, do you have your e-mail address on some of these lists to see what they're sending to make sure that they match on your relevance issue?

MR. TERRIBERRY: List industry is to a large extent based on trust. I've told people before that I sell a product that I never see, that I buy from people I never met, for other people I never met, that gets sent out by other people, that none of us ever met. And we get paid for it. It's a little spooky. But with e-mail -- and we're working kind of in two different markets. Most of what I do is business-to-business. And if you're sending a message to subscribers to meetings and conventions because you've got a meeting planning seminar that you're going to be running, meetings and conventions is going to look at that e-mail, they're going to vet the e-mail and decide whether or not it's appropriate for their subscribers before they'll even accept it.

MR. WENGER: Right. So, the list owner --

MR. TERRIBERRY: If they do --

MR. WENGER: Look at the advertisement.

MR. TERRIBERRY: -- anything that's deceptive --

MR. WENGER: Right.

MR. TERRIBERRY: -- the difference is that the owners that I'm talking about have no desire to see people unsubscribe, and if they deceive their subscribers, they're going to lose them. They're also sending publications of their own to those lists.

MR. WENGER: Right.

MR. TERRIBERRY: That maintains the value.

MR. WENGER: Right, so the list has value to it because people are wiling to accept what is being sent --

MR. TERRIBERRY: Right.

MR. WENGER: --- and so if you --

MR. TERRIBERRY: And they have them vetted as appropriate for what's being sent. As a list broker, yes, I do investigate the lists that I recommend to my clients.

MR. WENGER: Okay, thank you. We have a question over here, Sheryl.

MR. LEWIS: Yeah, my name is Chris Lewis, I'm with Nortel Networks. A couple numbers that I have that may be of interest to the panel, we have a pretty large mail system. We're running a large corporate mail system.

MR. WENGER: Maybe we could have him step up to this microphone here actually, because he's so close to it anyway, and then I wouldn't have to repeat what he

says.

MR. LEWIS: Okay, how's that?

MR. WENGER: The one to your left there.

MR. LEWIS: The other one, okay.

(Laughter).

MR. LEWIS: My name's Chris Lewis, I'm with Nortel Networks, I'm going to be on a panel tomorrow. I've got a couple of numbers that will be of direct relevance to what was just talked about today, but I'm not going to be talking about my economics session tomorrow. And that is there was a comment today or just recently about how it appears that harvested e-mail addresses disappear quickly from spam.

And our experience is the exact opposite. As a very good example, we had a series of domains that we de-registered, or actually we de-MXed, technically. It means we made it unreachable. You could not send mail to this anymore. At the time we turned it off, two and a half years ago, it was receiving between 60,000 and 70,000 pieces of spam a day. Out of curiosity, I turned it back on again two months ago, and it was at 600,000 per day.

These are addresses that were completely and totally undeliverable for over a year. And it went from 50,000 to 600,000.

MR. SMITH: Can I make one comment here?

MR. WENGER: If you speak into the microphone.

MR. SMITH: I think that what the CDT study showed is that if those -- any addresses still appear on websites then they'll still get spam.

MR. LEWIS: Oh, these have been administratively terminated through everything, because that is our corporate face, is those domain names. The other comment I wanted to make was -- is to stress the issue of dictionary attacks. I mean, people were talking about that today and they were talking about hundreds of thousands. I just wanted to mention that we have a series of undoing 6 to 7 million per day, and we're blocking entire countries because of this. This is how bad it's getting. Thanks.

MR. WENGER: Okay, I'd love to take more questions. I see more hands out there, but I'm being told that we're done here. So, I have -- I'm going to turn the microphone over to Renard Francois for a brief announcement, and then we'll see you back here at 1:30.

MR. FRANCOIS: Before you all leave, we have several important announcements to make, and I will try and do them as quickly as possible. First, name tags, if you are a panelist or an audience member, you should hang onto your name tags; panelists for the duration of the

forum; audience members for the day. So, if you go out to lunch, please bring your name tags, otherwise you will have to sign up and get new ones. But whether you are panelists or audience members, you will still have to go through security if you exit the building, okay?

Second, capacity. It's still first-come, first-serve with the chairs. And once we hit capacity, we will be turning people away and directing them to the overflow rooms, which I'm told has copious amounts of space. There are about 20 people in each overflow room, and we've corrected the problems that 432 is experiencing with audio. Even if your belongings are in here and we've reached capacity, there is -- we still won't be able to accommodate you.

MR. WENGER: So people should take their belongings?

MR. FRANCOIS: Yes. Camera lights. We know for people over here we've received some complaints about the camera lights, those are C-Span lights. We're told that if they remove them they will not be able to get the audience, so we apologize for the inconvenience, but they're going to be there.

This is for the media. Interviews cannot be done in the galley, which is the hallway behind the center; cannot be done in the conference lobby and cannot

be done in the building lobby. They can be done in the green room and outside of the building, as long as it doesn't obstruct the entranceway. If you have any questions, you can see Brian, Sheryl or myself or Mona or Voni.

MR. WENGER: Anybody with a green.

MR. FRANCOIS: Right. The other thing is temperature. We've heard other complaints about temperatures. As an addition, if you think this is cold, you should come to a commission hearing.

(Laughter).

MR. FRANCOIS: But we've been told that it will neither go up nor down, so for tomorrow, pack a sweater.

Page 2 of the bios, some people didn't receive page 2. Those are outside on the registration table. And the last thing is we will have Senator Charles Schumer coming in at about -- at approximately 1:30 to deliver some comments. The next panel will start shortly thereafter, it's Falsity in Spam.

Thank you.

MR. WENGER: Okay, thanks, everybody, for coming, and we're going to be starting sharply at 1:30, so please be back in your seats at that point. Thank you.

(Whereupon, a lunch recess was taken.)

AFTERNOON SESSION

- - - - -

MS. HARRINGTON: Good afternoon. We're back. A couple of announcements quickly before we turn to Senator Schumer. If you've got your cell phone on, turn it off, or we'll send you wireless SPAM. Remember that in the unlikely event of an evacuation, just go out the door. And that covers the security stuff. You also have to keep your badge on for the duration, or you'll go through sort of security purgatory to get in.

We are so lucky to have Senator Schumer with us this afternoon. He has worked closely with the Federal Trade Commission in his capacity as a member of the Senate Judiciary Committee. And most recently we were delighted to have him involved in the discussion of the Commission's generic drug study. He has long been a tireless advocate for consumers. And as many of you know, he has recently been discussing possible legislative solutions to the burden that consumers are confronting in their e-mail boxes.

And, so, without any further ado, the Senior Senator from the State of New York, the Honorable Charles Schumer. Thank you.

(Applause).

SENATOR SCHUMER: Thank you, Eileen. Well, thank you. It's good to be here with everybody, and first, before I get into the substance of my remarks, I

do want to tell you that I hope my speech today goes a little better than one I gave back in my old former Congressional District, the 9th CD in Brooklyn, because at the end of my speech, one of the senior citizen activists who populate the 9th CD in big numbers came over to me and she said, Senator, I thought your speech was absolutely superfluous.

(Laughter).

SENATOR SCHUMER: Well, I didn't want to let that remark go unanswered, so I responded. I said, Thank you very much, ma'am, I plan to publish it posthumously.

(Laughter).

SENATOR SCHUMER: But the senior citizen activists always get the last word in in the old 9th CD. She put her hands on her rotund hips, she waved her finger in the air and said, Senator, I just can't wait.

(Laughter).

SENATOR SCHUMER: So, I hope today what I have to say is not superfluous. I doubt it will be published posthumously or otherwise, but I'm very glad to be here to give you some brief remarks.

And first I would say to all of you that we are under siege. Armies of on-line marketers have over-run e-mail inboxes across the country with advertisements for herbal remedies and get-rich-quick schemes and

pornography. The Spam forum taking place here over the next three days comes not a moment too soon as we decide how to organize our counter-attack.

And I want to commend the FTC and Eileen Harrington, in particular, wherever she went, there you are, for bringing us here today. It is my hope that the impressive roster of panelists and speakers that you'll listen to and discuss issues with will stimulate ideas on how to stop the Spammers in their tracks. I have a number of thoughts of my own over the next few weeks and months that I'll be pursuing in Congress.

Now, as you are all aware, Spam traffic is growing at a geometric rate, causing the super-highway to enter a state of virtual gridlock. What was a simple annoyance last year has become a major concern this year, and could cripple one of the greatest inventions of the 20th Century next year, literally next year, if nothing is done.

Way back in 1999, the average e-mail user received just 40 pieces of unsolicited commercial e-mail, what we call SPAM, each year. This year, the number is expected to pass 2,500. I know I'm lucky if I don't get 40 pieces of SPAM every couple of days. As a result, a revolution against SPAM is brewing as the epidemic of junk e-mail exacts an ever-increasing toll on families,

businesses and the economy.

And let me illustrate this point with a personal story. My wife and I have two wonderful children, one of whom is about to complete her first year at college. The other, age 14, she's an absolute whiz on the internet. She loves sending and receiving e-mail. She spends far more time at the computer than she does watching television, which, in general, is a great advance.

As parents, we do our best to make sure she has good values and that the internet is a positive experience for her, a device to help her with her schoolwork or learn about events taking place around the world and maybe even a way to order the latest 'N Sync CD. But you can imagine my anger and dismay when I discovered that not only was she a victim of SPAM like myself, but like all e-mail users, much of the junk mail she was receiving advertised pornographic websites. I was and remain powerless to prevent such garbage from reaching my daughter's inbox.

The frustration I feel in the battle against Spam is one that I think business owners and ISPs across the nation can identify with. According to Ferris Research, Spam cost businesses in the United States $10 billion each year in lost productivity, consumption of

information technology resources and help desk time. With surveys showing that over 40 percent of e-mail traffic qualifies as Spam, we all know that ISPs spend millions of dollars each year on research, filtering software and new servers to deal with the ever-expanding volume of junk e-mail being sent through their pipes. They're doing a good job, but you know in this battle of offensive and defensive warfare, I'm afraid the Spammers always get a leg ahead and figure out a way around the filter. And that's why it's time for the Federal Government to step in.

And I was utterly amazed to learn, when I started looking into this, that Spamming is not a crime, unless you commit fraud, like everywhere else. And, so, over the next couple of weeks, I'll be unveiling a series of bills to clamp down on junk e-mail. And the legislation we will introduce will have two new weapons in the battle against Spam.

First, a Federal no-Spam registry modeled on the FTC's recently introduced do-not-call list. And second, for the first time, tough criminal penalties for repeat violators of new Spam regulations. Maintained by the FTC, the no-Spam registry will be a gigantic data base of people who have opted out of receiving Spam by submitting their e-mail addresses to the list. The model

for this innovation are the do-not-call registries that have been used to ward off telemarketers.

The FTC has just inaugurated its national no-call registry and expects telemarketing calls to decrease 80 percent as a result. We've had one in my State of New York. We signed up early on, and instead of at dinner jumping up, you know, like jack rabbits every three minutes to answer the phone, it has not ended these kind of calls, but it's curtailed them.

Now, critics have raised doubt about the registry, arguing it violates free speech or that it really doesn't prevent Spammers from sending e-mails, and it creates the very thing Spammers cherish most, a precious list of millions of e-mail addresses to which they can peddle their wares. Let me be clear, under my plan, Spam will refer exclusively to unsolicited commercial communication. That is a category of speech that doesn't qualify for full First Amendment protection, and it's been successfully regulated numerous times over.

And any Spammer that sends e-mail to addresses in the registry will be committing a crime punishable by stiff fines and potential jail time down the road. They don't get jail time; you first get a warning; you keep doing it in large magnitude, fines of up to $5,000 per day; and you keep doing if after that, it's jail time up

to two years. Now, these are the same devices we use to prevent more traditional crimes.

Meanwhile, the data base will be protected by military-caliber encryption, so that its valuable contents won't fall into the wrong hands. The list will be salted with dummy addresses, so that in the unlikely event that a Spammer cracks its protective codes and uses its content, FTC officials will be able to track down the offender and subject the Spammer to criminal prosecution for felony theft of Federal property.

Is it easier to go after the telemarketers than the Spammers? Yes. But there's one fact that underlines our enforcement effort, and I think that is key, and that's true with everything in terms of enforcement, and that is that 90 percent of Spam, 90 percent, is just sent by 150 spammers. So, that it's a small number who are doing most -- creating most of the problem. And as you'll see, we give the FTC the resources to go after those people, and that's how we can succeed here. We won't stop all of it, but this registry will stop a whole lot of it, particularly the big guys who do most of the damage.

Now, we also give the right for the FTC, state attorneys and ISPs to seek civil penalties against Spammers for the amounts of damages, I said, up to $5,000

per offense. But of equal importance, the FTC is going to have the funds needed to carry out this new mission. The no-spam registry and tough enforcement measures will not become unfunded mandates.

Originally, someone proposed that we put $75 million in this, which Congress would gladly allocate to get rid of spam, but we heard that's more than 50 percent of the whole FTC budget already, so it will probably be less than that, but money, Eileen, money will be no object.

(Laughter).

SENATOR SCHUMER: You'll be able to do whatever you need. Now, my plan doesn't stop there, although that's the heart of it.

MS. HARRINGTON: That's the most important part of it.

(Laughter).

SENATOR SCHUMER: That's right. And, by the way, again, free speech objection, not to a telemarketing registry, because you have the right to say you don't want to hear, see, get something in the mail. That's completely consistent with the First Amendment and of course we're dealing with commercial speech anyway.

But here are some other things we do. In addition to the two central provisions of criminal

penalty and the registry, we're going to take aim at mass collection of e-mail addresses and the rampant fraud, which, according to a report released by the FTC, is present in 66 percent of junk mail. My legislation will ban the hated practice of e-mail address harvesting, affording internet service, chat room participants and news group users a new level of protection from Spambots.

Subject headings, headers, domain names and router information of commercial e-mail will have to accurately reflect the content and source of the messages. All commercial e-mail will have the letters ADV, capital ADV, in the subject line, indicating that it contains a message with commercial content. The ADV heading, of course, is particularly useful because it will allow filters to easily separate the spam from the personal or business-related e-mail users receive each day. And any commercial e-mail without a valid unsubscribed address will be considered illegal.

The skeptic, of course, will say that all of these are great ideas but hard to implement in practice, especially given that the internet makes sending spam incredibly inexpensive and easily anonymous. That's why at the heart of this legislation are the tough penalties and the enforcement dollars. Yes, it will take a while to chase these folks down, but again, because 90 percent

is sent by 150 Spammers, you go after the big ones, keep them on the run and we'll make a real dent here. We will really make a dramatic, dramatic difference.

So, as you can see, this is a comprehensive plan. It addresses the technical problems associated with stopping Spam in its tracks; provides effective enforcement mechanisms to end this insidious fraud and harassment by peddlers of pornography, financial scams and deceptive advertising. And I fully expect it to turn the tide in our battle against spam.

I should add if you're a legitimate company, you'll have nothing to fear from this legislation. Indeed, I believe you should get on board as one of its chief advocates, because right now people are so frustrated at the junk e-mail bombardment that they delete everything, including legitimate commercial e-mail, as if it were spam. Implementing these rules means it's more likely your message will be read.

I hope this plan provides you all with fruitful fodder during your discussion over the next couple of days. I am interested in your feedback. If any of you have other ideas, ways to improve what we're doing, we're just at the beginning here, I'm a member of Judiciary Committee. It's Judiciary and Commerce that have joint jurisdiction over this. We welcome them, and please

don't be shy. You will be able to send us an idea by e-mail, by calling us, by whatever, and we will try to incorporate them. So, contact my office if you have other ideas.

I'm excited about the upcoming legislation, and knowing the wide public distaste for spam, I believe that support from other members of Capitol Hill will be forthcoming. I'd be very, very surprised if we didn't pass a comprehensive anti-Spamming bill this session of Congress.

Thank you very much.

(Applause).

MR. COHEN: Thank you. Well, Senator Schumer will be a hard act to follow, but we'll try. Welcome to the Falsity in Sending of Spam panel. My name is Stephen Cohen. I am a Staff Attorney in the Division of Marketing Practices at the Federal Trade Commission.

With me on the panel today is Margot Koschier, who is the Manager of the Anti-Spam Analysis and Prevention Team at AOL. Chris Jay Hoofnagle is the Deputy Counsel of the Electronic Privacy Information Center. Bryan Bell is the Senior Abuse Investigator at MCI. William Plante is Director of Worldwide Security & Brand Protection at Symantec. Samuel Simon is Chairman of the Telecommunications Research & Action Center. And

Scott Richter is President of Optinrealbig.com.

We're going to start out this session with Margot doing a presentation on falsifying header information and spoofing.

MS. KOSCHIER: Okay, everybody, thank you for the introduction. I have been asked to do a brief technical introduction into what the technical specifications of e-mail falsification are. And in order for you to adequately understand those, you need to know what is good -- what are good headers from what are bad headers. You need to be able to draw that distinction. So, we'll do basically an intro to e-mail, what TCP/IP, DNS and SMTP are, and then I will do a forgery of an e-mail.

Okay, TCP/IP is transmission control protocol/internet protocol. It's the language used by machines, of which the internet is composed. Each machine is connected to each other to communicate with one another. IP is responsible for moving packets of data between the servers and nodes; and TCP is responsible for verifying data delivery from client to server. Client is a term that refers to a freestanding machine that acts on another machine. The server is the one that serves it with data.

If you have more questions -- this is like

30,000-foot level here, in this dog-and-pony show, so if you have more questions, I refer you to www.rfc-editor.org. RFC 791 and 793 will go into more detail on that. And at the bottom of each one of these slides, if there are relevant RFCs, I put the basic ones on there, so for your knowledge.

Okay, IP addresses are coordinates used to locate where servers on the internet are with respect to each other. Every machine connected to the internet has an IP address, and I apologize if this is like common knowledge, but I just want to bring everybody to the same base level here. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods, for example, 208.15.23.1. Each set of numbers is termed an octet or net block, and each octet can be 0 to 255, so 256 characters potentially. RFC 791 has more information on that.

DNS. Domain name system is a distributed internet directory which associates a domain name, like aol.com or ftc.gov, and the IP addresses of the servers which belong to that domain name. Most internet services rely on DNS to work, and if DNS fails, websites can't be located and e-mail delivery stalls. Good tools to help you determine which IP addresses are associated with which domain names and vice versa are NS Lookup and Trace

Route from a networked Unix host.

And if you don't have that kind of access to your mail servers, your systems administrators are a little more protective and I encourage you to go to www.samspade.org or mayeast, which is a really long URL. I think my thingy here, my slide show's up on the website, so if you need it, you can get it from there. Trace Route and NS Lookup are on those websites.

SMTP, simple mail transfer protocol, is the procedure which generally happens on port 25, by which e-mail data packets are transferred from one machine to another. They are thousands of different types of software which speak SMTP. Some software packages are free; others are not. SendMail is the most widely used, available software. It's virtually free and pretty darn reliable. And then I list some other software products. RFCs 821 and 822 talk about the creation and formulation of an SMTP transaction.

Okay, here's an SMTP example. Matthew from Brightmail came up and did a presentation a bit ago on his harvesting tool and you saw little pieces of an SMTP transaction in there. Here's another one. Basically I said Telnet, which is on port 23, to Yahoo's mail server on port 25. I connected to it. Over here, I said, Hi, I'm from aol.com, because I was. He said, Okay, this is

my name. I said, I want to send mail from mkosch@aol.net, which is one of my e-mail addresses, to testforftc@yahoo.com, which is an e-mail address I created for illustrative purposes today.

They said, Okay, the recipient, testforftc@yahoo.com exists. I said, Okay, now I'm going to send my data. He responded, 345, okay, go ahead. And then I typed in the date, April 28th, which was the time of the test from me; the subject; and then I ended the transaction with a period on a line by itself, and it said, 250, okay, I don't know what dirdel is, if somebody wants to tell me, I'd be -- Miles Linear in the audience?

Okay, cool, delivery. And then I quit out; and he said okay, bye-bye. So, if we take a look at that actual header on the mail, here's my test mailbox. Wow, this is pretty slow. You guys ever think about AOL Broadband?

(Laughter).

MS. KOSCHIER: Okay, this is not the full message, but let's take a look at the full headers here. And come on, little guy. Here we go. Headers, as I will talk about in a second, are stamped in the order in which the packet is received to machine. So, the bottom-most header line, which is this received from, is technically where it originated. So, I was actually signed on to

that IP address. That was my helo string. Remember, I typed helo, aol.com. And then I connected to Yahoo mail server, and then the mail connected to Yahoo and was delivered to the mailbox.

My from address, I said I was mkosch@aol.net, Margot, and the X apparently to -- who it was to was testforftc. Pretty straightforward.

Okay. Headers are the mess of received from lines, I just showed at the top, or bottom, of an e-mail message, depending on which client you're looking at. They are a recorded log of the specific route a particular e-mail took from its destination to its arrival point. Theoretically, they're stamped by every machine an e-mail packet hits in order from bottom to top. As we will find out in the next panel on proxies and open relays, sometimes headers aren't stamped. There are tricky things that you can do to outwit machines.

So, theoretically, the topmost received line in the header is the last machine an e-mail touched before it arrived in your mailbox. One thing to remember is since you don't have any pre-existing knowledge about where an e-mail went before it got to your system, the only header information that is reliable is the IP address that is connecting to your mail server to send that mail. Everything else could be totally faked and

forged.

And, let me just show you those headers. Here's how easy it is to forge an e-mail. What I'm doing now, if I'm still connected to my internal network, I might have been booted. Yep, okay, I'm not -- obviously having typing problems. I'm doing an NS Lookup like I specified before. I'm saying I want the mail servers for yahoo.com. Here are their mail servers, right here. So I'm going to telnet to one of them, on port 25. I'm connected. Helo, senate. Oops, sendate.gov, okay, sorry. Let's see, e-mail from -- who would be a good person to forge? Timothy Muris.

(Laughter).

MS. KOSCHIER: At ftc.gov. Resp 2, test for -- uh-huh, typo, okay. They're not open relays, everybody, take a look at that, relaying denied. No surprise from Yahoo. Test for FTC -- chalk it up to nervousness. All right. Cool. Here's where I say data. I'll do the date. Let's say it's August 13, 2024. From tmuris@ftc.gov. Subject, anyone know where I can buy some spurs?

(Laughter).

MS. KOSCHIER: Yeah, this is a test. All righty. This user doesn't have a Yahoo account. Testforftc@yahoo.com. That's surprising. I could have

sworn I have a Yahoo account. Test for -- did I spell it wrong? Oh, okay. Do that again, I'm sorry, gang.

Indeed I could have. Helo, ftc.gov, mail from, okay, data, date, Margot. Cool, we're done. Let's get out of there. All right, so it wasn't as easy as I thought it was going to be, but as soon as Yahoo decides to deliver the mail, we'll see that in my inbox. I have e-mail from -- good presentation from Yahoo.com. All right, who's the punk in the audience?

(Laughter).

MS. KOSCHIER: All righty. A good presentation. That's really funny, gang. Ha, ha, ha. Okay, if we take a look at the other one, on to more serious things, we've got a mail from some kluged e-mail address, still looking for spurs. And if we take a look at the headers of it, it's from tmuris@ftc.gov. You can still see the connecting IP address, like I indicated before, that's really the only reliable information of where this transaction is coming from.

I just happen to be logged in to our internal network at AOL to send this message, because that's the only way I can get to a Unix prompt, but it's extremely easy to forge header information. I really encourage you to take a close look at headers, see if the FTC -- take a look at samspade.org, see if the FTC has any kind of

authoritative answer with 152.163, and you're going to see that it's not, it's AOL, obviously there's something fishy there. So, that's pretty much what I have.

MR. COHEN: Thank you, Margot. And thank you to the Yahoo guys.

(Applause).

MR. COHEN: So, my first question is to all of our panelists, after seeing this, is why was e-mail designed to make it so easy to forge identities. Anyone who wants to answer that?

MR. BELL: Well, I will. It was back when the protocol was designed, security, forging and what they're going to do with e-mail nowadays was not thought into the protocol.

MR. COHEN: Any other thoughts? Sam?

MR. SIMON: Just a point, there was an ethic a long time ago that commercial -- I mean, it was designed when commercial e-mail wasn't even part of the internet. The whole idea of the internet was to be for the sharing of ideas among people and colleagues. And what the internet has become is certainly not even close. You know, you could use a variety of adjectives, compared to what it was originally intended to be.

MR. COHEN: This is a question for Bryan, Margot and Scott. What portion of the e-mail industry

uses falsity in their spam, such as false subject lines and false removal representations?

MR. BELL: Well, about 60 percent of the complaints that we get at MCI have either false headers, false e-mail addresses or deceptive subject lines, or a combination of all three.

MR. COHEN: Scott, do you have anything?

MR. RICHTER: No, I wouldn't have any comment on that. I don't do that, so I really can't answer.

MR. COHEN: Well, but in your experience with other bulk e-mailers, do you have any idea?

MR. RICHTER: No, I've never seen any statistics on that.

MR. COHEN: What percentage of spam -- this is also for the same group -- of spam have falsified routing information?

MR. BELL: I'd go back to my previous statement. It's hard, you know, about 60 percent have one of the three in the actual e-mail headers, falsifying information.

MR. PLANTE: If I could just add one comment.

MR. COHEN: Sure.

MR. PLANTE: Speaking to the Symantec experience, it used to be maybe six months to 12 months ago when we began investigating spams that involved a

Symantec product that it was relatively easy to trace who was sending it and in some way or other interdicted, especially if it were, in our particular case, a counterfeited material.

In the last several months, the spammers that are using this type of technique are becoming more and more sophisticated in their ability to cloak themselves. And as the early presenter mentioned about using samspade.org, that's not quite the effective mechanism that it used to be, because it's becoming easier and easier for people, if they are technically sophisticated, to hide themselves.

MR. COHEN: Well, what are the harms to consumers as a result of falsity in spam?

MR. PLANTE: I can answer that.

MR. COHEN: Yeah, you and Sam.

MR. PLANTE: Again, speaking from Symantec's perspective --

MR. COHEN: Also to businesses.

MR. PLANTE: And to businesses in general. In its most benign form, I think spam is just a heinous inconvenience. I mean, certainly, any consumer can tell you that getting a few e-mails once in a while that was unsolicited might be annoying, but when you're starting to deal with 50 to 100, and we are hearing of people that

are dealing with that type of numbers on a daily basis, that starts to impact business productivity to the individual employee. But when you're talking about some of the subject matter in the content of some of these e-mails, I mean, it smacks perhaps in some cases of sexual harassing environment, work environment. There is some question about that.

But then also the fact of the matter is that there is a criminal association with some of the people that are trying to get you to do something by opening and acting on their spam that, again, a couple of years ago didn't exist. We've talked to people that have again tried to buy a Norton product that in fact was sold through spam that have either got product that didn't work and we can't support it, because we didn't sell it, it's not our product, and about one out of ten tends to sometimes share these e-mails are in fact credit card scams. So, it's a wide problem, just on that one experience.

MR. COHEN: Sam?

MR. SIMON: It's hard to over-state how, you know, bothersome spam, per se, is to people now, and it's not just bothersome. In fact, I would object to the whole idea that spam is simply an innocuous inconvenience to people to put up with. If it ever was, it is now much

more than that. It destroys the value of e-mail which was and still is the killer app of the internet. It is becoming virtually useless to many, many consumers.

The falsity of routing, per se, if we want to just focus on that little bit, at one time in life, one could spend some of their time to respond back and say spam, go to samspade or find out who it is from and notify their ISP, and you get a few pieces of spam and you'd spend 15 minutes doing that. Now, it's just impossible to do. Even if you could find it, it doesn't matter, there simply isn't enough time in the day if anybody cared to do that, and it ought not to be their responsibility to have to do it. People want e-mail to communicate with people and for reasons that they want to.

Now, if you want to go to the -- and I'm not sure -- on the simple mistitling of e-mail, I think that that -- and we have -- had put a website called banthespam.org or .com, asking people to submit to us their experiences and how they'd been impacted by e-mail and it -- you know, there's some really good stories that we're getting and we have copies of that available. People are -- again, I almost get emotional about it, about the idea that you open a piece of e-mail because of the wrong -- because of a header that has what would in

anybody's term be illegal pornography.

And I want to read just -- I have one comment from some -- one of the comments from one of our people who submitted a complaint. And it goes like this, "I can no longer open my e-mail if any of my children or grandchildren are now in the room. The so called junk mail is more than anyone wants to deal with, but the pornographic material is wrong. I choose not to buy pornography for my home. I don't purchase pornographic material to come in my mail. Why should I have to be subjected to it in my e-mail? It should be my personal choice and not forced onto my computer and into my home." And it's from a grandmother who gave permission to use her name, Mary Field.

This goes to not just the content but the fact that she wouldn't know, when she opened it, inherently what was in it. And, so, here is a person, a grandmother, who says I can't even have children or grandchildren in my room when I open my e-mail because she has no idea inherently what's going to be in that e-mail when they open it.

So, I think consumers are being damaged enormously. In fact, the entire value of e-mail is being weakened, if not destroyed, by not just the spam but the way it's being done, that's the falsity of the

information.

MR. COHEN: So, that actually goes into what was going to be my next question, which was how does the falsity -- how is it affecting how consumers are viewing the rest -- you know, all of their e-mail. And I think you've spoken to that.

Chris, do you have anything?

MR. HOOFNAGLE: Sure, not exactly on falsity, but I think the percentage of spam that we're seeing now is pushing people out of participation in public fora, and we're seeing so many commercial messages on the internet that people are engaging in address concealment and otherwise leaving public fora and speaking on ideas of public concern because of the amount of commercial speech that is out there that is suppressing it.

MR. COHEN: William, did you want to add anything?

MR. PLANTE: Yeah, sure. Again, when we deal with some of our consumer and our consumer complaints, the first thing that we're concerned about again as a corporation is the misuse of our name in advertising product that in fact is not our product. You know, the value of Symantec's name in terms of goodwill is in the millions and millions of dollars, and when I have to -- not just write to individual consumers periodically,

because they have some virulent complaints, but to the presidents of corporations who are enterprise clients who want to understand why they're getting so much spam that advertises our product, that's a very serious concern, and that goes up to our boardroom, what are we doing about it, are we diligent enough about it.

And, so, I have two different departments whose responsibility is trying to fight both piracy and counterfeiting, which is a problem, but also now spam. I don't know that we're necessarily unique in that area either. But then lastly, we've had to get to the point of suggesting to people that they simply don't even open up unsolicited commercial e-mail, that there's an inherent danger to the point of, as the other speaker was mentioning with the grandmother, that you can't open it anymore without some fear of danger. And especially when you're talking about some of the pornographic e-mail that comes across.

I have kids, too, and they're not supposed to get on my machine, but by golly, once in a while, you know, it's a fast-speed machine and they're going to get on it. And, so, yeah, not only just in terms of consumers but for enterprise, for businesses, this has been a real problem for us, and falsity is in so many manifest ways a business threat and an affront to

individual morals.

MR. SIMON: Can I add something?

MR. COHEN: Sure.

MR. SIMON: There is the other part, there are some commercial e-mails I would like to get. I mean, I will occasionally sign up from businesses that I do team-business with that I would like to be able to receive that. And I think, not just me personally, but I think other consumers it is an efficient way of communication; it's a way to get specials if you're a good customer; and by both the amount and the falsity and the distrust that is created, it is making those legitimate uses of e-mail by valid commercial enterprises less valuable and less likely to be successful.

MR. COHEN: Do you see consumers being afraid that the e-mail they're getting is, you know, somehow false, sort of leaching over into other areas of the internet, thus making them concerned about their personal privacy or security in conducting transactions? Anyone?

MS. KOSCHIER: One thing that's come to our attention, if I might jump in here, specifically the forgery in the return path of the message oftentimes leads to denial of service attacks for the legitimate owner of that mailbox. If a spammer is initiating a spam run and uses tmuris@ftc.gov in the return path of the

mail, like I just did, and half the recipients that he's sending this spam run to are invalid, all that bounce mail is going to go back to tmuris@ftc.gov.

We get phone calls on a weekly basis from people saying I can't into my mailbox or our systems are shutting down, please, help us out. It's a real big problem. The consumer fears his safety. He wonders if there will be retribution taken on him by parties who think that he sent the spam in the first place. It's a real concern.

MR. SIMON: We also have a second experience in two weeks now where e-mail was sent out using a jacked domain name, and it happens that it was advertising Norton product, and this poor business -- in both cases it was a relatively small business. They were saying I'm getting all these returned e-mails and what's going on here.

So, the first problem is you have a business that starts being crippled and its own good name is compromised because somebody's jacking their e-mail address -- or, sorry, their domain name and spoofing off e-mails. And it's pure profit for the Spammer that is doing that. And then you get some guy who's got to tell his client base that A, I didn't send this; and, B, they've got to deal with all these returned addresses and

complaints. So, again, when we're talking about the potential negative impact to businesses, that, from our experience, is becoming an increased risk in using the e-mail and the internet.

MR. SIMON: We actually have a real live person who wrote and said that, "A Spammer recently sent out UCE with forged sender information indicating that I sent mail from a personal mail account I maintained. I suffered a deluge wherein thousands of bounced e-mails, death threats, complaints and removal requests in the short span of time it took me to notice and disable the e-mail account." And that was from David McKnett.

MR. COHEN: Thank you. Scott, do you have any info on what percentage of spam is spoofed?

MR. RICHTER: I can really only speak on my own inbox. Based on the spam I get, I'd say more than a third. Unfortunately, there's no central clearing house for e-mail, so, you know, I think the numbers are unknown.

MR. COHEN: Is that consistent with your experience?

MR. BELL: Well, our experience at MCI is it's a higher number than that, probably 60 percent have something that's forged in the actual headers itself.

MR. COHEN: Margot?

MS. KOSCHIER: It's difficult for us to quantify -- to come up with a quantitative value for what percent of e-mail is forged. I mean, considering we're dealing with billions of messages a day. Really a lot.

(Laughter).

MS. KOSCHIER: Not an insignificant portion. Enough to have a panel at the FTC consortium about it.

MR. COHEN: Well, and what are consequences to a spoofing victim, other than the ones that we've talked about?

MR. RICHTER: They need to notify the local police authority if they're getting death threats, like she just said occurred.

MS. KOSCHIER: Sometimes a campaign spoof that is mimicking a legitimate click here to receive your special offers or click here to get your instant greeting from your friend, it leads to a web page, which this is all spoofing, leads to a web page, which then downloads a trojan or some such unknown executable onto this person's computer, and then their security is really compromised. Sometimes their personal information gets mailed out via this automated program.

MR. SIMON: Well, just the problem with spoofing is not only the person's e-mail spoof, but it is part of this process by which you are encouraged to open

because you may be thinking you're getting mail from someone you know or someone important or the Chairman of the FTC, for example, and so it is part of what gets people to open it. And that again means they're exposed to information. Not just information, but potentially dangerous or unwanted things that they otherwise wouldn't even look at. So, it's both sides, not only the person whose name or e-mail account's been expropriated, but then the people who, because they think they know who's sending it, are encouraged to open the e-mail.

MR. COHEN: Is there any legitimate reasons for engaging in spoofing, trying to maintain anonymity?

MR. HOOFNAGLE: I wanted to address that point. I think this is the main point I wanted to make today, is that anonymity is a fundamental right tied to free expression, the ability to participate in political processes and the ability to share our ideas without suppression from either public or private censors.

So, I think it's critically important that people can still remain anonymous on the internet. So, to the extent they are -- and send messages to people without revealing their identity. I think we have to remember that any model that we choose to take here in the United States is likely to be copied in other countries, as well. And if you take relative privacy out

of the internet, it will have substantial consequences for those who live in countries without a First Amendment, for instance.

But our country has a long history of protecting anonymity in allowing individuals to engage in deception when there are -- in their roles as speaking as political speakers. And that tradition has been upheld all the way through just last year, when Watch Tower Bible was decided by the Supreme Court, which upheld the right for individuals to go door-to-door pamphleting about their religious beliefs in a community without having to identify themselves first.

MR. COHEN: But you wouldn't use the same criteria for commercial speech, would you?

MR. HOOFNAGLE: I think it's very important that if you are to write legislation to somehow prohibit the falsification of routing information that it not in any way impinge upon political expression, and I think we've seen a bill introduced -- excuse me, passed -- yesterday in Virginia that would prohibit those who send over 10,000 messages with some type of falsification in the header.

And I think we have to think very -- we have to think very thoroughly over whether a law like that could be applied to one of the very important list

servers that you or I might be one, whether it's David Farber's list serve or Declan McCullagh's list serve. These list serves have well over 10,000 members, and if there is an ability to, let's say, post anonymously or otherwise if there is some falsification in the header we have to ensure that this political speech is not prosecuted as spam.

MR. COHEN: I've had an e-mail request that the speakers identify themselves when they answer our questions, so if you could try and do that, I would appreciate it.

I have a question for Margot and Bryan, something we've been wondering about at the FTC. How do Spammers select the domain names or e-mail addresses that they will spoof?

MS. KOSCHIER: Okay, this is Margot. Sometimes it depends on the weather; sometimes it depends on the particular campaign they're engaging in. If they are taking an actual product and spoofing it, they might very well use the legitimate product's domain name or IP addresses. It really depends on the type of Spammer.

MR. BELL: Bryan here. Our experience has been it's one of two things. It's usually just randomly choosing a domain; or we have actually seen Spammers go after specific people and forge their domains for

whatever reason, most likely that they've made the Spammer mad and are trying to get back at the actual individual.

MR. COHEN: Other than the political speech issue, I'm wondering whether there are any beneficial purposes to allowing false routing or sender information. Sam or William?

MR. SIMON: This is Sam. I can't think of one.

MR. PLANTE: I also agree. Absolutely no way can this be a beneficial thing for businesses.

MR. COHEN: Should there be legislative prohibitions on the forging of e-mail sender or routing information?

MR. SIMON: I would fully support -- I thought Senator Schumer made a really interesting set of provisions, and I would definitely make it -- and being focused and I appreciate the concerns about free speech, and I think we do have to be careful, and I think the best way to be careful is to aggressively eliminate the amount of commercial spam, so it doesn't force more Draconion measures.

But I think legislation -- I think the Federal Trade Commission itself and just to remind TRAC and two other consumer groups filed a petition in September of last year. We believe the Commission could, on its own,

through enforcement, I believe it's filed a case against a pornographer in which one of the grounds was the falsity of the routing and spam. I think we need to go after it aggressively now, not wait. The legislative process can sometimes be delayed. The sooner you act, the better.

MR. COHEN: All right, well, let me ask the question the other way. Does anyone think there should not be legislation prohibiting the forging of sending false e-mail header information or routing information?

MR. PLANTE: Don't look at me.

MR. COHEN: Anyone. Just checking, no? Okay, great. Anyone have any ideas what can be done to prevent spoofing? Chris?

MR. HOOFNAGLE: I have an idea. It's actually opposite of an idea to prevent. But, you know, year after year in looking at privacy issues we see groups, whether it's the government or in this industry consortiums try to solve various problems on the internet, whether it's spoofing, whether it's digital rights management and copyright issues, whether it's facilitating e-commerce or otherwise trying to accomplish some business goal.

Every year we see a new idea of trying to install a system of trust or the idea of a trusted sender

or a network of trusted senders. I think that would be a bad way to try to stop spoofing and other types of fraud on the internet, because it will subject us all to being identified before we send e-mail.

MR. COHEN: Anyone else have any ideas?

Question for everyone. Is most spam -- we heard Senator Schumer say that most spam is sent by a small number of people. Is that actually true? Do we have any information on that? Scott, do you have any information?

MR. RICHTER: No, I was actually wondering where he got that statistic from.

MR. COHEN: No? Okay. Here's a question that we've been wondering about. What time of day or week is most spam sent, and why?

MS. KOSCHIER: I actually have an answer for that one. It's when we're not working. We find that most of the -- with respect to how many recipients per message arrive at our system, most of the high-recipient-per-message mail is sent between the hours of 11:00 p.m. and 5:36 a.m. in the morning, particularly heavy on Fridays and weekends.

MR. SIMON: It's our experience that a lot comes to people Sunday night. There is this phenomenon of people showing up to work Monday morning and usually

the first thing they do is open their e-mail and look at what came in and there is -- and this is almost conventional wisdom in persuasion e-mail and non-commercial e-mail that send out as to, you know, have it sitting in somebody's e-mail Monday morning, because that's when they're going to -- that's one of the first things they do when they come to work.

MR. COHEN: Scott, when do you send most of your --

MR. RICHTER: We've actually -- well --

MR. COHEN: Sorry.

MR. RICHTER: We've actually -- I mean, we have some mail that goes at all different times, depending on the customer's request, but we actually find that we have better results if we send during the day than trying to send in the middle of the night or, you know, different hours.

MR. COHEN: Is there any cost factor that would affect the decision as to whether to send it during the day or at night?

MR. RICHTER: Basically we just usually leave that up to the customer as to like what time they want to send out.

MR. COHEN: Anybody else? Let's see. Anyone have any idea what percentage of spam is now using

foreign servers? Does that seem to be a problem?

MR. PLANTE: Again, when we first started our anti-spam program, we found a fairly even percentage of U.S. domestic servers and foreign servers that were using our product name. We're finding a shift in ratio, maybe toward 60, 65 percent now, coming from foreign servers, which from our perspective makes it much more difficult to deal with when you're sometimes talking non-English languages, and so it's much more problematic for us. I think it's a shifting, at least in our experience higher. William Plante.

MR. COHEN: Thank you.

MS. KOSCHIER: This is Margot. We've noticed a trend recently where IP addresses that are registered to entities overseas or domestic that have been dormant for a while are apparently being misappropriated and borrowed -- we're terming these zombie net blocks -- for spamming uses. We're not quite sure how it's happening; we have a couple of theories, but mail is coming from places where it hasn't been coming from all along and these IP addresses are somehow being routed by -- the routes are being accepted by internet service providers, locally, domestically, but the IP blocks a long time ago should have been registered to folks overseas.

MR. COHEN: Could part of the problem be that

they've been sublet to other users?

MS. KOSCHIER: Could be, from what we've been seeing; however, it would indicate that the owners of these, the rightful owners of these net blocks, have no idea that this is happening.

MR. COHEN: Scott, I have a question for you.

MR. RICHTER: Yeah.

MR. COHEN: I hope I didn't put you on edge. Are senders of e-mail actually selling their own products? Or do they send e-mails on behalf of other clients?

MR. RICHTER: I think that would probably be depending on each individual company that sends mail. We have our own products, as well as we have customer products, but we're mainly sending products on behalf of our customers.

MR. COHEN: I've been asked to make sure that everyone speaks in the mike when they respond.

Scott, in your experience, who writes the text of the e-mail messages?

MR. RICHTER: Most of our advertisers have ad agencies who do their ads for them and their credos. They usually send over a couple different credos to see which ones have better responses and different things like that, but we usually leave that up to the

advertiser.

MR. COHEN: Does that include the subject lines?

MR. RICHTER: Yes. We don't usually pick a subject line for a customer; usually they'll give it to us, what they would like to use with their ad. If we find something that, you know, is misappropriate, we'll notify them.

MR. COHEN: How do you determine what is misappropriate?

MR. RICHTER: Basically we would look at the offer and, you know, take it from a case-to-case basis.

MR. COHEN: So you actually look at the offer and you look at the subject line and you look to see if they're related?

MR. RICHTER: Correct.

MR. COHEN: And what happens if they're not?

MR. RICHTER: Then it's usually the job of the salesperson to go back to the ad agency who sent us the job and go over with them, you know, something that would be more appropriate or, you know, something that we think would, you know, work.

MR. COHEN: Do you have any experience with others in the industry who might have different practices?

MR. RICHTER: I -- you know, I have some -- you know, I think I've read some stuff, you know, and I probably, you know, from what I read on chat boards and different things, but as far as the practices that we follow compared to what another company does, I really can't speak on their behalf.

MR. COHEN: Bryan, how many spam complaints do ISPs receive every day?

MR. BELL: Well, from our experience it averages about 7,500 complaints, and that is mass mail, web packing and use-net complaints. Bryan Bell.

MR. COHEN: Margot?

MS. KOSCHIER: Millions.

MR. COHEN: Millions per day?

MS. KOSCHIER: Millions per day. This is a good thing, though, because that means we know -- we know what our members find objectionable and we can take immediate action on it.

MR. COHEN: But do you find that with the spam complaints you're receiving now that a lot of your members are just clicking "notify AOL, this is spam," since that's the only option when they click that, because there isn't a, you know, notify AOL, I just want to unsubscribe because I'm 13 years old and my mom told me, because she's read every day on the news and media

and ads that do not click on subscribe links?

MS. KOSCHIER: I think the button on the bottom of the screen that says "report spam" is very clear that it means report spam.

MR. PLANTE: Again, if I may for a moment.

MR. COHEN: Sure.

MR. PLANTE: William Plante here. About six months ago, we started our spam watch at Symantec.com, and after a few weeks we're getting maybe a couple hundred, maybe 300 complaints in one day. And these are e-mails from consumers that do not have any ability to directly click a button and report this to us. They have to find that e-mail address. As of Monday, we are now averaging 1,500 to 1,600 e-mail complaints a day. Again, that's just on our product-specific stuff, for people that have to hunt the e-mail address down.

So, again, going back to some of the earlier comments, I think that people are becoming more and more frustrated and looking for ways to complain about it. So, that's just been our experience. A lot more people are becoming vocal about it.

MR. SIMON: And if I could add, this is Sam. I think that most people don't -- you know, I think AOL's button is great. I think most people, though, who are on either a corporate or a generic e-mail service don't know

what to do; A, B, don't do it because it doesn't make any difference. And, you know, I love the uce@ftc.gov where I was for a while, but I gave up, because nothing happened. You don't get a recognition, there's no sense of results, and I think people just give up filing complaints when there is no feedback or no impact of the complaint being filed.

MR. COHEN: Well, the FTC receives, I believe, 170,000 UCE per day. It would be impossible for us to respond to each one of them. We have over 11 million spam in our spam data base. We do use the spam data base. It is very important to us. We use it as part of our investigations and it has been very helpful in bringing a number of cases. So, I would, you know, urge people to continue to forward their spam to the FTC.

MR. SIMON: I didn't mean it as a criticism as much an indication that whatever reports going on is probably only a small fraction of the actual feeling and complaints that are out there.

MR. RICHTER: A big problem I notice is that as an example, and they're not up here, but Yahoo several weeks ago launched a contest and, you know, that the more e-mail that you want to report as spam you'll be entered to win prizes. And I believe that a lot of people are reporting spam, or you know, that may not be spam,

because they're being enticed to do it. I personally reported all my friends to try and win a free year of Yahoo.

(Laughter).

MR. COHEN: You'll let us know if you win, right?

MR. RICHTER: No, but, I mean, what I'm trying to say is you can entice somebody and get -- I mean, if somebody wants to report spam, I think that's great, they should. But if you're promoting it as a contest or, you know, as in a different way where it may be -- you know, maybe they really did receive it, but unfortunately like with somebody like Yahoo, there's no way to respond. We don't know how many people click "this is spam" to enter the contest. And maybe it isn't spam, how do -- you know, and there is no way for us to respond and say no, this is one you did opt in. This is one you did confirm your e-mail address; this is, you know, when you visit our website. There's -- and that's a big problem with the industry, is that the people who send the mail don't have those opportunities.

MS. KOSCHIER: I can tell you from experience in looking at complaints that the marketing organizations whose domain names reflect the information that's in the headers do generate fewer complaints than those who have

anonymous information or random characters inserted into the from addresses. The cleanliness of headers does make an impact on how members view the mail.

MR. HOOFNAGLE: This is Chris from EPIC. I think the ultimate enticement, I mean, aside from games to entice people to report spam is actually to create a law that has a private right of action so that individuals can actually get satisfaction for spam. And we currently have this framework in the telephone and consumer protection act of 1991, a law that gives individuals a private right of action in their local state court, and there is an entire bar of people who litigate under this law. And as a result, the junk faxes and other annoyances that that law was designed to prevent have gone down significantly.

MR. COHEN: A while back the FTC did a remove-me surf, in which it found that 63 percent of unsubscribe links did not work. My question is what percentage of consumers actually try to unsubscribe from lists. Does anyone have any information about that?

MR. RICHTER: Was that a -- when you say 63 percent of them didn't work, was that current e-mail you received, or was that e-mail that you may have received six months previously and, you know, an ISP decided to, you know, terminate an account or -- I mean, there's -- I

think there are some issues or factors that could go behind whether a remove address works.

MR. COHEN: That was within one to two months.

MR. RICHTER: Okay. And one thing that makes it -- one thing that we've always done a good job of is always making sure that each piece of e-mail that we send has always a minimum of two ways to unsubscribe, usually a web-based unsubscribe, as well as they can respond to the e-mail with a remove. And we also have some where we've experimented using call-in numbers or a postal address, but, you know, basically the first two seem to work the best.

Unfortunately, you know, there could be, you know, instances where a black group, you know, tries to do collateral damage or, you know, tries to force you off an internet service provider's band width and it's, you know, out of your control if removing doesn't work or doesn't, you know, work for a period of time.

MR. COHEN: Do you test the remove links from your e-mails?

MR. RICHTER: Yes. Yes. We'll add ourselves to lists. We'll, you know, add two addresses, not confirm one and confirm the other; you know, get two e-mails, unsubscribe from one, make sure we don't get a second one. We're constantly, you know, testing and

trying to do things that would, you know, ensure that everything works.

MR. SIMON: This is Sam Simon. Part of the problem right now is -- well, there are many problems, but most -- one I would like to point out is that there is a conflict of public information. If you watch a typical consumer news show, a consumer reporter, they'll do a story and say yeah, the remove things now do work most of the time and it's an urban myth that they're using this to harvest e-mails. And you'll turn to the next station and it will give you the exact opposite advice, that no, anytime you hit the remove me, that's just a scam to show that you have a real e-mail address.

And consumers don't know what to do. Even if yours worked, people don't know what to do, and by and large, wouldn't dare use them because they're afraid that this is testing the validity. But they get contrary information. I don't think people know reliably what to do about the remove buttons, to try them or not.

MR. COHEN: Is there any empirical evidence for the proposition that by trying to remove yourself you're actually confirming your e-mail address? Because that has not been the experience of the FTC.

MR. RICHTER: No, that's --

MR. COHEN: We've actually tested for this.

MR. RICHTER: That's, I think, an urban myth. I'm sure there was somebody who did that, but, I mean, one thing like with us, as a practice we have, why would you want to send to people who don't want e-mail? I mean, that would be -- if somebody removes themself from your list, if they've joined your list and then they remove themself, it would seem unpractical to continue to want to send to somebody like that.

MR. COHEN: Do you have -- while you're speaking, Scott, do you have any information as to why Spammers, not yourself, I'm not talking about you.

(Laughter).

MR. COHEN: Because I wouldn't call you that. Why those people include removal links if they do not work? What would be the purpose of doing that?

MR. RICHTER: You know, I would really have no idea why they would. I mean, to me, like in most spam that I receive, I don't ever see a remove link and, you know, I mean, the less things in your e-mail I think that you put, say, the word unsubscribe, remove and different things, I think, you know, helps them to be filtering, so I think it definitely plays against us by having two remove links in every e-mail we send.

MR. COHEN: Do you think it adds to the legitimacy of the e-mail if there's a remove-me link?

MR. RICHTER: Yeah, I think it's -- well, I think the key -- things that make an e-mail more legitimate, one is you send from a real domain name, that's your domain; you get bounces, you're not -- you know, nobody is going to get your bounce or it's not spoofed or forged. Everybody, you know, anybody can identify the information, the headers, as, you know, who it came from.

MR. COHEN: Does anyone else want to speak as to whether it adds legitimacy to the e-mail?

MR. PLANTE: Yeah, William here again with Symantec. About three weeks ago, we had an incident that involved a fellow who one of my investigators had direct contact with and felt compelled to contact me on, where he spent just over two hours going through all of the e-mail filtering folder that he had and started unsubscribing. And having done that, he was compelled eventually to drop that e-mail address completely.

Now, that's anecdotally. I can't give you an empirical statistic, but I can tell you that if the choice is, you know, content filtering and sending the stuff off to a folder and/or going up and opting out, I would just as soon delete and try and deal with it in terms of a volume problem every couple of days going through a folder and deleting it.

This guy was just so distraught. He was extremely angry. Not at us. And I can't even recall how my investigator came into contact with him, but he was looking for some help, and all we could ever tell him was just delete the stuff, don't even open it, and we're sorry to hear that it happened to you.

MR. SIMON: I actually have a real-life note here, actually from Robert Helt, who's a senior technical specialist, information system at General Mills, who said that as a senior technical specialist in a Fortune 100 company I have seen the effect on productivity of landslide of spam -- the landslide of spam has caused. We tried to filter to block; changed e-mail addresses; and various other countermeasures, but it still gets through. Trying to, quote, opt out, or quote, unsubscribe, just makes it worse.

MR. COHEN: Are there any questions from the audience? Lots of questions from the audience.

(Laughter).

MR. COHEN: Brian?

MR. HUSEMAN: I wanted to follow up on one thing. Excuse me. AOL tells its members to not unsubscribe from e-mail, in AOL 8.0. And I was just wondering what your basis for telling your members that was.

MR. COHEN: Margot, will you repeat the question?

MS. KOSCHIER: The question was we allegedly instruct our members not to attempt to unsubscribe themselves from e-mails. And that is not true. At keyword postmaster or keyword mail controls, I believe keyword post -- actually, it's keyword junk e-mail now, we say look at the e-mail, treat it suspiciously, if you believe that your unsubscribe request will be honored, by all means, go ahead and unsubscribe. If you have any doubt, don't. We leave it to the member to decide.

MR. COHEN: Gentleman in the back? Please identify yourself.

(Question not audible from audience).

MR. COHEN: So, the question -- the point was that web bugs might be contained on HTML pages and that by opening up the link or the message that's in the e-mail, it sends back a notification that the e-mail address is valid.

Gentleman here.

AUDIENCE MEMBER (Partially audible): The question I want of the panel, my company sends permission-based e-mail on behalf of our members, so in the e-mail headers, we will actually have the return address of our member who's sending it or whom we are

sending it on behalf of; however, on the e-mail headers, it will show our IP address as the originating e-mail server. Would that be considered false --

MR. COHEN: So, the question is when you're sending e-mail on behalf of your marketers, the information shows that it is coming from you when it actually might be coming from someone else. Is that correct?

AUDIENCE MEMBER (Partially audible): -- it has our member's return address in it.

MR. COHEN: Oh, it has your member's return address?

AUDIENCE MEMBER: Right, if it is coming from them. We are just sending it for them.

MR. COHEN: Okay.

AUDIENCE MEMBER (Partially audible): The e-mail itself is coming from our servers; however, we put the member, our member's e-mail address in the from line.

MR. COHEN: So, if we were tracing it, it would come back to your server.

AUDIENCE MEMBER: Yes.

MR. COHEN: But if we looked at the e-mail -- the IP address on the e-mail, it would have somebody else's server.

AUDIENCE MEMBER: -- first return address is

his machine.

MR. COHEN: Right.

MR. SIMON: Well, TRAC in this position -- it would be my position that the real party in the interest of any commercial e-mail should be identified correctly. And it doesn't really bother me where it might be, but if it were in the text of the e-mail, with a valid phone number, as well as e-mail address, that would be enough for us.

MR. COHEN: Please introduce yourself.

MR. SCHOKEL: I'm Brad Schokel (phonetic) with AAC&G.org, which is our user group association of computer users. One of the questions I'd like to address would be the validity of the unsubscribe address. I'm a member of the task force that analyzes spam, we have been for several years now. And when we test the -- I don't know how FTC tests it, other than sending mail to them, but we also looked them up in the WhoIs and called the telephone numbers and then called the city where they reside and so forth.

And the big problem we found in the way we separate it out, who might be a valid unsubscribe address and who might not be, which who hasn't falsified their whois information? And generally speaking, we're only finding 17,000 pieces of spam we analyzed, there were

like 37 which were valid. Okay? And the thing of it is, when you go back to the whois, that's really the only way is the owner of the domain. And most of those are either rows of Xs or they're completely erroneous telephone numbers, like to a vacant lot in New York, something like that. And, so, that's really the only way you have to track back the owner of that domain.

The other thing I'd like to address, too, is the foreign ports thing. There seems to be a disparity in data or people not understanding the percentages on that. But that is like doubling every two or three weeks -- (inaudible). And in terms of identifying 150, what the Senator was talking about, there -- I think he has really accurate information. We actually have about 225 IP blocks who consistently send spam, but through our network off other user groups who have their own mail servers, who are sending their logs, we've analyzed logs from all over the country. It seems like no legitimate mail is coming from these numbers. So, it's sort of like if they're only serving spam and there's no legitimate mail -- (inaudible) -- then they have to be Spammers.

MR. COHEN: Okay.

BRAD SCHOKEL: I only wanted to make that point.

MR. COHEN: Thank you. The issue -- it's a

very interesting point about comparing the whois information to the unsubscribe information. About a year or so ago the FTC sent a letter to ICANN and it's the Bureau of Consumer Protection, I believe, recommending that the whois information should be accurate, because consumers rely on that information and it is important that the information be accurate. And this shows why.

AUDIENCE MEMBER: They just passed an initiative, too, just about two weeks. They finally passed an initiative at ICANN to cause registrars -- we need somebody here from ICANN. Is anybody here from ICANN?

MR. COHEN: All right, well --

AUDIENCE MEMBER: Have the registrars check once a year the validity, and if it's not valid, they block that domain.

MR. COHEN: Thanks, Mona.

MR. RADEN: Some of the leading e-mail software packages now have preview panes in which they actually open up the e-mail for you automatically, if you will. Now, if web bugs are, in fact, one of the ways that they validate your addresses, is there anything, short of closing the preview panes, that the consumer can do, the recipient can do? And I'm David Raden from the Post Gazette and Megabyte Minute Radio.

MR. HOOFNAGLE: I think there is. There's filtering you can do to disable HTML as you receive it in your mailbox. I don't want to promote certain products, but I think it's worth looking at Spam Assassin and some of the front-ends for that program that will turn off HTML e-mail.

And some spam software itself will let you disable spam -- excuse me -- some e-mail software itself will let you disable HTML as you receive --

AUDIENCE MEMBER: (Inaudible) -- using the product itself that you know of, short of shutting down the -- (inaudible).

MR. HOOFNAGLE: I don't know the whole line of products well enough to answer that question.

MR. COHEN: Would the panelists say it is deceptive for a remove-me link to take the recipient off of only the list for that mailing, rather than from the list for all future mailings?

MS. KOSCHIER: I would think it would depend on what the remove-me link were advertising it would do.

MR. COHEN: Scott, do you have anything?

MR. RICHTER: I didn't really understand -- I mean, as far as remove them from the -- are you saying remove them from one e-mail or remove them from all future e-mails?

MR. COHEN: Remove them from one e-mail rather than all future e-mails?

MR. RICHTER: Why would they --

MR. COHEN: Would that be deceptive?

MR. RICHTER: Oh, I mean, anybody who clicks -- yeah, to me, yeah, and anybody who clicks with us would be removed from all future e-mails.

MS. FLANAGAN: Hi, my name is Erin Flanagan, I'm with Consumer Base. Everything that we were talking about or you were talking about in this panel is clearly fraudulent with forging headers and open relays and everything. And I never hear any distinction between any commercial -- like legitimate commercial marketers and like fraudulent Spammers. And I feel like commercial marketers are constantly being grouped in the same category, but I don't think that we do anything fraudulent, yet we get treated like some porno Spammer. So, how are you ever going to differentiate between a legitimate marketing company and some spam operation out of somebody's basement?

MR. COHEN: The question is how does one differentiate between commercial -- legitimate commercial e-mailers and Spammers.

MR. SIMON: This is Sam. I think my point earlier is that legitimate companies are among those who

are hurt the worst by this kind of spam, so you're endorsing effective remedies, banning together to get something done quickly would be a way to help yourself, A; B, there are a variety of viewpoints on whether there ought to be only opt-in. But assuming that there isn't an opt-in world, that it is an opt-out, I would say, and it is our view and the petition our group's filed would expect that any legitimate e-mailer would have an accurate description of the e-mail on the subject matter; an accurate identification of who sent it; how to reach those people in real time, as well as a valid unsubscribe element, all of that before we would consider it a legitimate marketing piece.

MR. PLANTE: William here with Symantec. Let me make one other point, that with our resellers and redistributors of our product, we have had discussions with them about the use of e-mail as a marketing tool, simply because we've been dealing with the spam problem now for several months, well, six months, actually, approximately. And it is so tainted, that mechanism, that medium, that although we don't have a contract with them, so they can't, but, you know, by verbal agreement they've acknowledged that they simply can't use it anymore because there's no validity to it.

MS. KOSCHIER: From an AOL perspective, I can

say that our determinations as an organization of which entities are Spammers and which are not, regardless of whether or not you consider them to be sketchy are based on what our members decide. It's complaint-driven in our perspective.

MR. COHEN: Okay. Sorry, go ahead.

MR. NOONAN: My name is Kevin Noonan, I'm the Executive Director of the Association for Interactive Marketing, and I just wanted to say that we've been working with a lot of these ISPs, and I believe that AOL and a lot of them are doing a great job in trying to combat this.

I also wanted to congratulate CNET, who I receive e-mails every day from, and sometimes don't open them for a period of a week or two, and after about a two-week period, my investor CNET newsletter wasn't opened, and they actually sent me another e-mail saying we've noticed that you haven't opened this for some time, do you wish to remain on our subscribe list, and if you do, then just let us know, and if we don't hear from you, we'll take you off that list. And I think on the other side of the fence, that's a very positive thing to do. And my question would be to the panel, is there any evidence of the newer TLD, the top-level domains, of being more egregious Spammers than the dot-coms out

there.

MR. COHEN: The question is whether there's any evidence that the new TLDs are more egregious Spammers than the dot-coms. Anybody have any experience?

MR. SIMON: But there is so much. I mean, actually, there is so much out there and so frequent that it would be very hard to make that kind of judgment.

MR. COHEN: Questions? Anyone?

MS. LIEB: Rebecca Lieb with Internet.com. I wanted to make, if I may, two additional points on two items that were discussed during this panel that I think were perhaps overlooked. One was the material damage of spoofing to businesses. There was some discussion of brand and reputation damage. I think it's important to note that a number of companies have had to shut down operations or at least the IT aspect of their operations for several days in some instances after being bombarded by bounces and by complaints, effectively putting them out of business.

Secondly, on the unsubscribe, we've been hearing a lot about unsubscribe links in e-mail, but that's not necessarily been clarified. Sometimes unsubscribe links take you to a landing page where you can unsubscribe or you're automatically unsubscribed. But very often these links are in e-mail that

unsubscribes the address from which the e-mail was sent.

When e-mail addresses are illicitly harvested off websites, lots and lots of aliases are harvested along with them. Feedback@, webmast@, abuse@. Very often these aliases are distributed to dozens of people, none of whom can send an e-mail from that address to unsubscribe from anything they were subscribed to, which means a lot of stuff is effectively unsubscribable, given the current form.

MR. FOX: Jeff Fox, Consumer Reports. I just want to submit a little bit of evidence about the unsubscribe option. About 14 months ago, which I now regard as the good old days when most of our spam did not have forged headers, that's how much it's changed, I think, in the past year, we did a little experiment with some of the spam we were getting, repetitive spam coming from the same domains. And we unsubscribed to a couple dozen of them.

We published this about a year ago. Most of them stopped coming, you know, within a couple of weeks after we unsubscribed. But we noticed a few weeks later, some new e-mail started coming from domains which when we did a whois, coincidentally, happened to have the same registration address as some of the domains we'd unsubscribed from.

And, so, you know, nowadays with forged headers, this whole thing may be pointless, you may not be able to trace it anymore, but this was some evidence that the same companies would apparently unsubscribe you from, you know, It's-Amazing-Offers.com, or Big-Deals-For-You.com, and then, you know, a month or two later -- and the registration address of the new domain was often quite recent, and so for 10 or 20 bucks they can just take out a new domain. They can claim to be respecting your unsubscribe, and then if you don't know how to do a who is, you know, there they are Spamming you again under another name. So, this is some of the practices that go on.

MR. COHEN: One more question. Someone over there.

AUDIENCE MEMBER (Partially audible): Hi, I'm -- (inaudible) -- and I'd like to return to the question of anonymous speech. I get a lot of anonymous mail from deliberate anonymizing services. The best known is -- (inaudible) -- but they're all over the place. And what the headers in those messages say, this mail came from IT, we don't know where it came from before that, because we deliberately didn't record it. It seems to me that's a perfectly reasonable way for people who want to provide anonymous service to provide it. (Inaudible) -- I don't

see anything that's forged in that. I wonder whether the lawyers here would agree that this is -- it is possible to have mail that is anonymous without any kind of forgery.

MR. COHEN: Chris, do you want to respond?

MR. HOOFNAGLE: I'd like to speak about that. I mean, there are several different types of anonymous re-mailers, and I'd have to think about whether there could be -- whether what you say could be written into a law so as to affect the commercial senders and not affect the sending e-mail over the re-mailer. But I'll have to think about that.

AUDIENCE MEMBER: Well, a related question is is there such a thing as anonymous commercial speech? I would say that a business -- that the point of commercial speech is to get somebody to contact you and buy something --

MR. SIMON: This is Sam. I wanted to come back to that topic briefly, too. And I would first, on your point, I wouldn't think there's any valid anonymous commercial speech. I do think that the remedies are sensitive, and I think the idea of basing remedies simply on the numbers of e-mails are of concern, because there's -- increasingly e-mail is trying to be used in our political system, not just in advocacy, but if you -- as

we go into the next few presidential campaigns, you're seeing increasing numbers of both parties and candidates using, and if our test of what becomes spam -- unsolicited commercial e-mail is speech from political candidates, I think that that's a problem, and therefore, I think the solutions are difficult, although I think that aggressive prosecution, and I like the criminal prosecution piece of this, is important, it will hopefully scare away the worst offenders.

MR. COHEN: And we will have to end on that note. Thank you very much. We have a 15-minute break.

(Applause).

MR. FRANCOIS: We're going to go ahead and get started. This is panel number four of the day, dealing with open relays, open proxies and formmail scripts. We have a distinguished panel with us here today, and instead of two hours, we're going to hold it to about an hour and 45 minutes and reserve questions until the end.

Briefly, what this is about is we will discuss open relays and proxies, but in general, this deals with security issues where people who don't have the intention of sending voluminous amounts of spam to people actually end up sending voluminous amounts of spam to people. And, so, this is a topic that really touches on not just businesses that receive it, but businesses that may have

their systems that are not properly configured; individuals who maybe have home networks that are not properly configured, which allow Spammers to really manipulate the system to their advantage to, one, facilitate sending a large amount of e-mail messages without -- at no cost, but also allowing them to displace the burden and any type of adverse impact on people that have these security weaknesses.

So, we're going to jump around a little bit. We have several -- three presentations for you. One will be of open proxies; the other will be of open relays; and the final presentation, which will be at the end of the panel, will talk about new threats, new and emerging threats to security and which Spammers can exploit.

Then beyond that, after we do our first two demonstrations with proxies and relays, we will have a discussion about open relays, open proxies, honeypots, the international aspects of open relays and open proxies, new and emerging threats, as well, and then we will save some time for questions from the audience.

So, with that in mind, I will defer to our first panelist, Matt Sergeant from MessageLabs, who will give us a very brief presentation about open proxies. And then we will move to a PowerPoint presentation by Nick Nicholas, which will be addressing open relays.

After that, we'll jump into a general discussion of both open relays and open proxies.

MR. SERGEANT: Hi, I'm Matt Sergeant, the Senior Anti-Spam Technologist for MessageLabs. What I want to talk to you all about today is the problem of open proxies. And first of all, I want to really explain in very simple terms what an open proxy is, because this is a fairly recent threat that most people who deal with spam have dealt for a long time with the problem of open relays. And as such, the problem of open relays has been communicated extremely well to the general public, but perhaps a great number of people don't really know about the growing problem of open proxies. So, I want to explain today about how they work and why you might have one.

The picture here is to basically show that somebody at home might install a DSL connection, so they've got a permanent line to the internet, they've got a high-speed connection. And one of the things that we're seeing more and more of in recent times is that people want to build an internal network, and for this internal network, they want the other computers that they buy to be able to access the internet to browse the web and receive and send e-mail.

The thing about doing this with the regular

home DSL subscriptions is that the computer that you get that connects to the internet gets a public IP address, but the computers on your internal home network get a private IP address. So, here we've got a setup with three computers, one connected to the internet with a public address and two behind the internet connection with private IP addresses. And those two computers can communicate with each other within their own internal network, but by default, the usual situation is that they can't browse the web.

So, the person setting up this might go to google, usenet and type in how do I, you know, connect these computers to the internet? How do I get them to browse the web? And one answer that might come back would be to install a proxy server. So, they do this and they install the proxy server and now, by doing this, the computers behind the internal network can browse the web and use e-mail. So, that seems like a great situation for the person who's just created their home network.

But what they don't realize often is that these proxy servers are created in an insecure manner. They're installed by default open, so that the entire world can come in and use this proxy server to connect to the rest of the internet from that one connection. So, the Spammer or potential abuser, because this is not just a

problem for Spammers, open proxies are a source of various kinds of abuse, they come in, they connect to the proxy server installed behind somebody's DSL connection, and from that point they can browse the internet. And the reason that they do this is simply to hide where they're coming from.

The other reason that Spammers might do this is because there are a large number of these open proxies out there, so they can use this as a system whereby they can hop around all over the place, sending 100 e-mails from one, 100 e-mails from another and hopping around as quickly as possible. And they do that so that their source of e-mail doesn't get noticed. So, 100 e-mails from one particular host might quite easily fall under the radar and not get noticed by an incoming mail server. Whereas, you know, the total volume that they're sending, which might be millions of e-mails, certainly would get noticed. So, this allows them to hide and sneak around.

The way to secure an open proxy is very simple. You can either install a firewall or you can change the configuration of these proxy servers. It's as simple as that.

The problem with open proxies, though, is that unlike open relays, the owner of the open proxy never finds out that they have an open proxy. The machine

running the open proxy is not really designed to send e-mail in the same way that an open relay is. When you install an open relay, it's designed to be a mail server, so you expect to be sending mail out from it. And if that server ends up in an IP black list, you find out about it very quickly, hopefully, and you can do something about it.

With an open proxy, it's not designed to send e-mail, you just -- the DSL connection would mean that you are supposed to send e-mail through your ISP. So, if you had, for example, a Roadrunner connection, you would go through Roadrunner's SMTP servers, rather than sending direct to the recipient.

So, the owners of those open proxies, they don't get to find out that they've been blacklisted. They don't get to find out that they have an insecure system, so they can't fix them.

The other thing is that ISPs don't check these blacklists, so they have no way to detect whether their own customers have actually installed an open proxy. They -- most ISPs still aren't doing scanning of their customers to find these things, so they just -- they get set up and then they just remain there. So, the number of these open proxies is still on the increase. It's rapidly increasing. I think the number of open proxies

is doubling about every five or six months at the moment. So, it's a real problem.

Logs are nonexistent for these. They are home users. So, if you have a source of spam coming through an open proxy, you can find out the IP address of the open proxy, find out that it is an open proxy, but you can't find the real Spammer behind that, the Spammer's actual computer, because it's very difficult to go to a home user and say give me the logs. You know, it's much easier to go to a mail administrator and say that, because they would have procedures in place for maintaining those logs and backups and things like that, whereas a home user doesn't maintain that kind of thing and they will very often delete logs, reformat their hard disk and things like that.

And the final point is that end-users, they're really not sys-admins at the end of the day. So, they're not really that interested in fixing these problems. If you contact these home users and say excuse me, you have an open proxy installed on your system, they'll be like I don't know what you're talking about, because they don't really understand the problems here.

So, how does an open proxy work? I was actually going to try and do a demo of this, but the internet connection is not very good, so I'll just talk

through it. It's very, very simple to abuse an open proxy. Most of the spam-sending ratware out there now incorporates features to use open proxies directly. But from a very sort of low level, all you do is telnet to the open proxy on the port that the proxy is listening on, and you type connect and here I'm connecting to mail25.messagelabs.com, which is one of our mail servers, connecting to port 25, which is SMTP servers, and then you press return twice. And if you get a response from that that says 200 connected, which is the response you would get from an SMTP server if you successfully connect to it, you're free then to send e-mail direct to that SMTP server.

So, this is an incredibly simple way of doing abuse. There are a number of different types of open proxies which work slightly differently, but the premise is basically the same, and the software that is used to send spam wraps all of this up. So, you don't actually have to -- as a Spammer, you don't have to manually type any of this is, it's all done automatically for you.

And the final point there is that the IP address that you might be using to abuse the open proxy will not show up in the headers of the e-mail that gets received. So, it's a completely anonymous service that happens here.

How many open proxies are out there is a very difficult figure to try and estimate. We think at the moment there's somewhere in the region of 52-hundred-thousand. It seems to be a vaguely agreed-upon figure in the community. At the moment, as far as quantity of spam is concerned, last month in March we were seeing about 60 percent of all our incoming spam coming through open proxies. So, this is a huge chunk of the spam problem right here.

And the use of open proxies is increasing all the time. It's probably up to something like 65 or 70 percent for April.

How do Spammers find these open proxies? Two ways really. They will actually go out and they will port-scan IP addresses in networks that they know host DSL connections. So, they will go out to the Brazilian ISPs, who they know that they -- you know, they have these DSL connections and a lot of their users aren't terribly knowledgeable. They will go out to all the major U.S. ISPs who give out DSL connections.

And they will actually scan for them using specific software designed to find these proxy servers. And very much like we saw earlier in the demonstration of e-mail harvesting, you just get a list of these, which you can then plug into the ratware to send your spam out.

The second way is that some of the commercial ratware on the internet which you can pay for comes with a monthly subscription that you pay for and the provider will send you either monthly or weekly a predetermined list of open proxies that you can abuse. And this installs direct into the client, it's completely automated, you don't have to do any of the scanning yourself, and obviously it is a very powerful tool for anonymizing the e-mail for the Spammers.

Finally, how do we fix the problem? A big part of the open proxies problem is getting ISPs to take action for their customers. They -- we believe that ISPs need to start scanning their customers, finding out if they have these insecurities and getting their customers to fix the problem, and if they can't -- if they can't get the user to fix the problem, they really should be disconnected from the internet, because they are inflicting this abuse on the rest of us.

And the quote there is, you know, we don't want to drink their dirty water anymore; we'd rather they cleaned it up before inflicting it upon us.

Another thing that ISPs can do is they can check the public blocklists against their IP ranges, so they can go through these blocklists and say, do I have any customers listed in your blocklist, and if so, they

can then find out who the customer is and get the problem fixed.

And finally from a receiving end point of view, for those of us receiving spam, use of these DNS blocklists is extremely effective now against the spam problem. The open proxy blocklists are very targeted toward open proxies, and as such, they're very effective and have very, very low false positive rates, so that they're very useful.

And, finally, a question mark, because there are probably multiple solutions, and hopefully we can discuss some of those.

Do you want me to go and talk about formmails right now?

MR. FRANCOIS: Yeah, so that way the -- we can have a chance to switch the computers.

MR. SERGEANT: Okay.

MR. FRANCOIS: We're going to have Matt talk about formmail scripts and the inherent weaknesses in those that Spammers use, have used and exploited to send their spam.

MR. SERGEANT: Okay. I just knocked up one slide about formmail scripts. Formmail scripts actually aren't used very much in spam any more. They have seriously declined in popularity. We still see every now

and then some spam coming through that has abused a formmail script, but it's very much on the decline.

The formmail scripts are very simply scripts that have been downloaded from the internet for the purpose of building feedback forums on web pages. So, you would have a form on the web page that says please fill in your details and click submit and we'll send you some more information. And many websites have these kind of things.

The most common one that people have download is the one from Matt's Script Archive, called formmail.pl, and that's not me by the way, that's a different Matt. This script was originally developed around 1996 and was very insecure by default. It allowed people to come into the web page and send almost any content that they wanted through that script. So, you could -- this is another thing, very much like open proxies, a way to anonymize yourself so that it looks like the e-mail is coming from somewhere else.

The problem now has been mostly fixed. If you go now to the web page for Matt Script Archive, it says there are some security problems with formmail.pl and we recommend that you use the NMS version of this script.

So, there's a website there which seems to have faded out a bit in the presentation, but it's nms-cgi.

sourceforge.net.

And these are actually a bunch of friends of mine in London who sat in the pub one day and said you know, we're really sick of hearing about this formmail problem, let's fix it, let's get together and fix it. So, they've provided free equivalents that are secure by default for the formmail scripts and various other of Matt Scripts. So, you can go there and download that and fix the problem.

And that's about it for the formmail scripts.

MR. FRANCOIS: Thank you, Matt. Just a quick question, in terms of while this may not be a method that Spammers are using frequently, are there still -- what's the prevalence of the formmail scripts that are corrupted that are still out on the internet? Do you have any idea of what that might be?

MR. SERGEANT: It's a very difficult figure to test for. It seems that there have been a large number of downloads of the NMS equivalent, so hopefully the insecure ones are going away. I can't give you an exact figure, unfortunately.

MR. FRANCOIS: And maybe you can briefly kind of go into a little detail in terms of what was the specific problem with the formmail scripts that were being exploited.

MR. SERGEANT: Okay. The specific problem with formmail scripts was that the recipient e-mail address for where the contents of the form were to be sent was encoded directly in the web page. What this allowed is the -- somebody abusing the formmail script could construct their own web page containing a completely different recipient and a completely different set of content and post the results of that form through the script. And that would send all of that content to the falsified recipient and it would appear to come from the formmail web page.

MR. FRANCOIS: Was there any problem with Send Mail or Send Mail 8.8 or that's involved in formmail or is that another problem that I'm thinking of?

MR. SERGEANT: It's possibly another problem that you're thinking of. There was a slight -- there is a very small issue there in that Send Mail allows you to do rooting based on the -- a specific formatting of the e-mail address. And, so, when this issue first cropped up, Matt fixed the problem in formmail.pl, or so he thought, but it still allowed you to do what's called percent routing.

MR. FRANCOIS: What is that, if you could explain that a little bit?

MR. SERGEANT: It's a way of formatting an e-

mail address recipient. So, you say -- you can say that the recipient is supposed to be map%messagelabs.com@, and then the server. And Send Mail, although it looks like it should be going to a different server, Send Mail will kindly route it to the domain after the percent sign. So, formmail did a very simple check to see if the domain was in a valid list of domains, but it didn't check for the percent routing problem.

MR. FRANCOIS: All right. Now we're going to turn to -- jump out of water a little bit -- and turn to Michael Rathbun, who is with Allegiance Telecom in Texas, and to give us an overview of the arms race, so to speak, in spam, and where -- how we got started and where we are today and how we got there. We're going out of order, just to kind of give the computer folks a chance to change the computer so we can do the other demonstration, so that's why we're going out of order.

But, Michael?

MR. RATHBUN: Thanks, Renard. In 1995, I first encountered internet e-mail spam as a problem when it was being sent by a fellow in Seattle named Willie Newell (phonetic). And Willie had a product to sell that later had some suitability issues, but he basically buried anybody who was posting to usenet in those days with spam for the Zygon learning machine. And you might call him

the first large-volume but rather naive Spammer because he sat essentially on a T1 line, dedicated connection, to an ISP in Seattle and he sent out quite a bit of mail.

Well, the first thing that happens in a situation like that is the proprietors of systems who are being assaulted, thusly, noted the address from which the mail was coming and went to their routers or servers and did some typing and suddenly those IPs were no longer to deliver mail. And that was the first countermeasure that you saw against that kind of event.

A somewhat more sophisticated set of Spammers came along in late '95 and early '96 and became more agile, you might say. One particular famous Spammer had what he called a band width partners program where he would basically freight you a server; you plug it in, you turn it on, you're connected to your network and you ask no questions and you accept his check. Thus when people began adding his current IP addresses to their routers and servers, he would simply fire up his next band width partner and begin sending from that, until it, too, was blocked.

That measure promoted another countermeasure, largely -- essentially the ancestor of the blocking lists that we see today. A man named Paul Vixie was rather irritated at having to go and update lots of IP addresses

and various routers and various places, so he created a realtime blackhole list, which became quite popular with a number of system operators and whenever Paul would make an update to his list as to where Sanford Wallace or one of his other counterparts was sending from today, suddenly that IP address would vanish all over the place where anybody else who was accepting that feed was able to block those essentially in real time, as soon as Paul saw them coming in. Within half an hour, anybody who subscribed to that list was also protected.

That was sort of the death nail for that particular round of what I would call fixed-address Spamming. And these were people on high-speed lines with fixed IP addresses and the next obvious place to go was someplace where there were just millions of possible IP addresses you could send from, even if it was at low speed, and that was the vast number of dial-ups that were available. And at this particular time in history, I was working for a dial-up ISP provider and got involved in that particular series of events.

And what would happen in the most prolific cases is a Spammer with a stack of prepaid, precharged credit cards could sign up for, oh, two dozen, 300 or 400 different accounts at dial-up providers and use the dial-ups, connect a machine to that and just send away at 28.8

or whatever speed he could obtain. And if you had enough of these going at once, you might as well have a wide band connection.

So, that particular method inspired its own set of countermeasures. One of the first things that the dial-up providers began to do was to configure their systems so that when you're dialed in you cannot talk to a mail server that's outside the network that you belong to. You would be forced to send through your own server, because at that time, the folks using the dial-ups would use open relay servers, which you'll hear about shortly, as their preferred method for both concealing their origin and increasing their effective band width.

And, so, the dial-up ISPs began to do what is called port 25 blocking, which prevents the user of a dial-up account from communicating directly with an e-mail server, other than the one that belongs to the provider he's getting his connectivity through. And that was for a while a real curb on the use of dial-up accounts for Spamming.

However, it turns out for these countermeasures, there are counter-countermeasures, some very creative ones. One particularly prolific Spammer is known to use a system in which a single machine has both a broadband connection and a dial-up connection. And the

software inside has been hacked so that the packets to the receiving server go out on the high-speed connection, but inside the packet, the source address which says this is where this packet came from, and if you're going to reply to it, send it to this address. It happens to be the address of the dial-up side. So, it will go out the high-speed side and get replied to on the low-speed side. And this gets around the port 25 blocking problem and the fact that dial-ups aren't very fast.

There are various countermeasures to that that I can't discuss.

(Laughter).

MR. RATHBUN: The other thing that will take up a lot more of our time that Matt has already discussed that solves the problem of port 25 blocking for dial-up users is open proxies, because port 25 blocks port 25, which is the SMTP connection; whereas open proxies use any number of different possible input ports, and depending on what kind of service the proxy provides, it can end up coming out and talking to any number of different kinds of services, whether it be telnet or HTTP connections or SMTP connections or any number of other things.

Now, as Matt mentioned, there are for some providers the policy of going out and scanning the

customer's boxes to find out whether there's anything out there that's vulnerable. I know that Roadrunner does that; we do that as well. We don't have cable modem subscribers, but we do have lots and lots and lots of small businesses who may do any number of different things to do connection sharing.

And we see -- as in the month of February, we saw incidents of proxy abuse in our network. We received about 1,300 complaints.

MR. FRANCOIS: I hate to interrupt you, but I want you to hang on to those, because we're going to return to them when we talk about open proxies in a little further detail.

MR. RATHBUN: And the countermeasure to scanning and customer education, the latest vogue is the trojan proxy. We've begun to see these in our customer networks, in which they get infected with a piece of malicious software, which then installs a copy. In what case, the sobig.a --

MR. FRANCOIS: Well, hang on. We're going to talk about that, too. And things coming down the pike or that have already come down the pike, so --

MR. RATHBUN: Let that thunder not be stolen.

MR. FRANCOIS: Exactly. But now we're going to turn to Nick Nicholas, an internet consultant who is

going to talk to us about open relays.

MR. NICHOLAS: While I'm getting set up here, I'd just like to thank the staff at the Federal Trade Commission for inviting me to participate in this forum. I also would like to commend the FTC for looking at this very, very important issue, which as several other speakers today have noted, costs in the billions of dollars per year.

What I'm starting off here is just a few basic schematics, showing how a relay works. The first schematic shows the basic way an e-mail gets transmitted from point A to point B. Literally we have a customer of ISP A and they want to communicate with a customer over on ISP B. Is my pointer even reaching over there? No, I guess not. So much for my laser high-tech.

The mediating server is -- there's a server that mediates between the ISP A and the ISP B, and the customers of ISP B would actually communicate with their own ISP's mail server in order to receive the e-mail message. Now, it's possible, and Michael Rathbun has already alluded to this, it's possible for a customer to acquire software which will allow -- essentially turn -- instead of being at a normal workstation like this, you can actually replicate the functions of a mail server. And you can thereby bypass your ISP's mail server and

connect directly to the receiving ISP's mail server and there reach any of the customers on that end of the switch.

Now, this is the schematic that shows how an unsecured mail relay works. We're still a server here, and rather than connect directly, the reasons Michael has mentioned some of the reasons you might not want to do a direct connection, traceability is the main point. Find an unsecured mail server. These are rather easily found. There are Spammers out there who will sell you lists of unsecured mail servers. I think they go for about a dollar each. And if you want an anonymizing server, which will actually disguise the actual source of the mail, those go for about $2 a pop. So, the mail will actually go through the unsecured mail server and then onto the receiving ISP's mail server and thereon to all the fortunate recipients behind ISP B.

The final schematic I wanted to show actually combines the two tactics we've discussed so far. We've got ISP C down here now, and this little red machine here is an open proxy, and it is possible to chain an open proxy with an unsecured mail server and thereby disguise the actual source of the message. It will look like the message is actually originating from here, and in that way you'll get complete anonymity in what the actual

sources in the mail messages are.

Now, I was going to give a brief -- an actual how-to. Are there any Spammers in the audience? No real mail servers were used in this demonstration; no laws were broken; and most of all, do not try this at home. I picked up from a recent spam that I received a -- it was sent through an open relay, kension.plus.com, and you begin this process. Margot sort of stole my thunder by doing this same demonstration. You simply use a convenient utility called telnet, which allows you to remotely access machines, and that colon-25 on the end is important, because that's where the simple mail transport protocol is listening.

And it will respond with the message saying -- identifying itself, letting you know that it's ready to go. It will also tell you what mail transport agent is being used. And, so, I now say hello, misspelled helo. Now, I'm using some of the Spammer tricks in here, so this is actually overlapping a little bit with some of what was covered in the previous panel. Helo hotmail.com. Now, of course I'm not hotmail.com, but I want the receiving mail server to think that I am. And it will simply respond okay. It will accept whatever I tell it it is.

Then I tell it that I'm sending mail from

president@whitehouse.gov, and it will tell me that sender is okay, even though, of course, I'm not president@whitehouse.gov, at least not yet. Then you identify the recipient, this is all specified in the protocols, rcpttodrumsfeld@dod.gov, and it will say that that recipient is okay as well. Now, I enter data, and it will tell me it's ready for -- ready for me to go.

The first thing I'm going to do as a Spammer is put in some forged header information. I want the headers to reflect the fact that this really did come from hotmail, and I even did a little bit of homework. I found out that one of the IP addresses for mail.hotmail.com is in fact 65.54.254.129. And, so, I very carefully constructed this header, this particular data point, so that the recipients are going to be fooled by this, more than likely than not. This is still data -- what we put in the mail from doesn't necessarily have to reflect what's said here, but I am for convenience sake. To drumsfeld, subject, invasion of France.

(Laughter).

MR. NICHOLAS: Please proceed immediately with plan for invasion of France, G.W. Bush. And here's that tiny little period there that lets you know I'm done with the data part.

MR. FRANCOIS: You're going to get me in

trouble with the international panelists, and the international division.

(Laughter).

MR. NICHOLAS: I picked this for you.

MR. FRANCOIS: It's been a great job while I've had it.

(Laughter).

MR. NICHOLAS: And the period is important. The period tells you that you've concluded with the data section, and it's set. It says mail is queued for delivery. At this point I could identify new recipients, but instead I'm just going to quit and it signs off, closing connection, good bye. And it's really -- it's that easy. And that's why hundreds of Spammers, if not thousands, do it daily.

Just before closing out, I wanted to talk a little bit about the scope of the problem. It's actually an old problem. It's been a problem at least since 1996, but it is still a problem. The MAPS RSS has a little under 180,000 open relays listed. Another list run by Osirus Soft has over 190,000 listed. The open relay data base has 182,000 listed. DSBL has 214,000; and the NJABL, not just another bogus list, has 255,000 listed. There is some overlap between the lists, but not completely so.

Most of the experts think that we have at best half of the open relays identified. So that means that there are approximately half a million open relays out there that can be abused. The problem is not going away. I know of some ISPs that check incoming connections to see whether or not the mail server that's trying to make a connection is an open relay. I've heard from one ISP that they're finding 400 new open relays a day.

Mark, if I can put you on the spot for just a second, I know that Roadrunner does this, can you give me an estimate of how many open relays you're finding? Is 400 a conservative estimate?

MARK: Based upon the amount of mail we get, it's a conservative estimate.

MR. NICHOLAS: Four hundred is conservative.

MR. FRANCOIS: Mark in the audience said that 400,000?

MR. NICHOLAS: Four hundred new ones.

MR. FRANCOIS: Four hundred new ones is a conservative estimate.

MR. NICHOLAS: Every day.

MR. FRANCOIS: I just wanted to repeat that for the people listening.

AUDIENCE MEMBER: (Inaudible) -- we have more than that.

MR. NICHOLAS: You find more than 400 a day?

MR. FRANCOIS: What we're going to -- I'm sorry to cut you off, Nick, but we want to kind of save the questions and comments from the peanut gallery, so to speak.

MR. NICHOLAS: Okay, I just wanted to get some real world input. So, 400 is -- 400 new ones a day is a conservative estimate.

MR. FRANCOIS: Right.

MR. NICHOLAS: So, it is an old problem, as I say, but it's still a problem that's with us today.

MR. FRANCOIS: And I'm going to go ahead and kind of open up questions to the panelists about open relays and open proxies. We just heard that 400 new open relays a day -- does anybody have any information in terms of how much are getting put on blocklists a day or a week?

And if you could go ahead and identify yourself.

MR. NICHOLAS: Nick Nicholas again. Each of the relays are different; each of the lists are different. But it ranges from anywhere from as few as 50 a day to a couple hundred a day. And these blocking lists, though, are very effective in getting rid of -- getting some of these open relays closed. So, there's

quite a bit of turn in the number of relays that are open. So, they are getting closed, but as soon as some get closed, there are others being uncovered.

MR. FRANCOIS: Close anywhere from 50 to 200 a day, but --

MR. NICHOLAS: Correct.

MR. FRANCOIS: -- you're still getting at least 400 a day opened?

MR. NICHOLAS: Right. So, the problem is growing rather than shrinking.

MR. FRANCOIS: Is there any way -- oh, go ahead, I'm sorry, Matt.

MR. SERGEANT: For open proxies, the figure is about -- on average of about 2,000 a day, coming on-line.

MR. FRANCOIS: Two thousand being discovered?

MR. SERGEANT: New ones being detected.

MR. FRANCOIS: Detected? And likewise, the same question, how many are being put on blocklists a day in your estimate?

MR. SERGEANT: That data is based on blocklists.

MR. FRANCOIS: Okay. So, 2,000 coming up active and then afterwards, when they're discovered, how many get put on the list and deactivated, or can they be deactivated?

MR. SERGEANT: There is some evidence of slight decreases, but nothing nearly dramatic enough.

MR. FRANCOIS: Okay. In terms of open relays, I know that -- is it possible -- you gave a demonstration where there were forged headers, and one of my questions was whether that was done automatically or by hand, and if it's done by hand, by a particularly diligent Spammer, is there any way for a person who has received mail to track it through an open relay and to the originating source?

MR. NICHOLAS: I just did that by hand as a demonstration. There's actually software that automates that entire process and is able to do hundreds of thousands of these per hour, so it would be quite tedious to try to do a couple hundred thousand per hour by hand.

What was the second part of your question?

MR. FRANCOIS: The second part of the question was basically addressing --

MR. NICHOLAS: Oh, if you can -- you can't tell from the headers themselves whether it came from an open relay or an unsecured proxy. The headers themselves won't reveal that information. You'd actually have to scan the machine to see what ports were open. A good way to do that, without necessarily scanning the machines yourselves, is to check some of the lists -- I listed

five there -- and see if it's already been determined to be an open proxy or an open relay.

MR. FRANCOIS: Okay, but even if you send spam through an open relay and I trace it through the header, it won't eventually come back to you?

MR. NICHOLAS: Not necessarily. Not necessarily. There are anonymizing relays and especially if you do a chain process where you combine an open proxy with an unsecured relay, the chain will actually stop at the open proxy, and it will look as if the open proxy is the source of the message.

MR. FRANCOIS: A quick question about the number of potential ports that a proxy or an open proxy can be -- that can be exploited by an open proxy. Just a rough estimate of how many ports are out there and how many ports are available that can be exploited?

MR. SERGEANT: Well, theoretically, the total number of ports is about 65,000, but generally they tend to fall into specific ports for specific pieces of software, so you can actually go out and look specifically for port 8080, or port 1080, or something like that, for a specific type of proxy server. But more and more we're seeing open proxies appearing on randomized ports, which obviously is a much more difficult problem to deal with. That tends to be -- that

tends to fall into the area of trojans.

MR. FRANCOIS: I know that there's been a lot of numbers bandied about today, and probably for the rest of the forum, in terms of the amount of spam sent per day in relationship -- or the amount of e-mail sent per day. Is there any way or do you all have any evidence that indicates how much spam on a daily basis is sent through open relays and through open proxies, or as a matter of a percentage?

MR. PATTON: I would say through my own experience -- this is Brad Patton -- that recently, especially within the last few months, 40 to 50 percent of all the spam relayed to our network or through our network is done so using open proxies or open relays.

MR. FRANCOIS: Okay. Michael?

MR. RATHBUN: During the month of April, up until the 26th, looking at the just raw count of unique IP addresses involved in a spam sample of 4,571 addresses that had been tested during the month, 55.1 percent were already identified as open proxies on one or both of two different lists that were in use. So, the number's higher than that --

MR. NICHOLAS: I've actually heard numbers as high as 95 percent are being sent through unsecured proxies. Proxies seem to have overtaken relays in terms

of what kinds of systems are going to be abused.

MR. FRANCOIS: How recently has that --

MR. NICHOLAS: I would say this was within the last few months that they jumped to a number that's that high. Now, these are smaller systems that ISP administrators are reporting that as many as 95 percent of the spams they're receiving have already been listed on one of the open proxy lists.

MR. FRANCOIS: Okay. In terms of mail servers and open relays, are relays left open intentionally for spamming, unintentionally? Why does that --

MR. NICHOLAS: Well, that's a good question, actually. There are -- particularly in corporate environments, some corporations will leave their mail servers unsecured so that executives and sales folks who are on the road will be able to still use those mail servers, regardless of where they're dialing in from. Typically, you may be dialing in a dial-up at a hotel. And, so, they'll leave the home server, so to speak, open so that they sales folks or the executives won't have to make any changes in the configurations on their mail clients.

So, it's done largely as a matter of ease of use for certain corporate end-users. So, it does have a valid use. There are ways around that, though. that's

not necessarily the only way you can accomplish that end, but it's the simplest way, and some people want to go for the simplest solution possible.

MR. FRANCOIS: Is it also that the tools for authenticating users and access to the network have gotten so much better over time that there's really no need to leave a relay open?

MR. NICHOLAS: I would agree with that definitely.

MR. SERGEANT: Absolutely 100 percent. There is no technical reason now that you need an open relay.

MR. FRANCOIS: Can anybody proffer a reasonable reason for maintaining an open relay?

UNIDENTIFIED SPEAKER: I can't think of one in today's context, honestly, no.

MR. FRANCOIS: What about open proxies in terms of -- I know that there -- proxies serve a valid function, caching remote access and you've spoken a lot about the insecurities in them. Are the insecurities -- again, are they intentional? Are they unintentional? Is it a mistake of the user confusing -- trying to set up a web server and they make a mistake? Is it being shipped in the box that way?

MR. SERGEANT: I would say that 99.9 percent of the time it's unintentional. It seems that --

MR. FRANCOIS: And unintentional -- I'm sorry to cut you off -- and unintentional on whose part as well.

MR. SERGEANT: From the person who installed the proxy server. It's unintentional that it was set up insecurely. I'm sure if you were able to contact the people who were running them, they would probably be quite surprised and confused. Most of the software that does this seems to be set up by default to be insecure, and that's one of the biggest problems.

A number of people have actually spoken to the authors of these software packages to try and instigate some change there. And some of them have fixed the problems; and some of them are disinterested.

I'm sorry, there was another part of your question, as well.

MR. FRANCOIS: Yes, we just combined the parts, so you answered both of them. One other question about open proxies and open relays. What is -- I guess all the people that contact individuals that are operating open proxies and open relays, what has been generally their response? Is it shock, amazement and cooperation or indifference?

MR. PATTON: I would say through my experience it would be bewilderment and they don't really believe

that so much mail has been sent from their network or through their network, but it's usually, once you get the person calmed down, or explain exactly what's going on, it's usually a simple fix. It's just a misconfiguration of the actual software, and if you can explain it to them, normally it takes about 10, 15 minutes to resolve the issue.

MR. FRANCOIS: Adam?

MR. BROWER: I'd like to interject. My name is Adam Brower, by the way, I'm a citizen of the United States. I'd like to interject kind of a sociological note, and that's really why I'm here. I don't pretend to have the technical expertise of some of the other participants, but I've had some experience dealing with administrators in other cultures, and in particular in Asia I found that the concept that an unsolicited approach to business -- it's hard to make the point initially that it's unwelcome, because in Mayan cultures, it's honored, it's considered a very polite thing to do, and it's an honor to be so requested and so solicited.

And I must say that kind of goes along with what Brad was talking about, amazement, that bewilderment is not only technical and not only evidenced by, you know, raised eyebrows and I can't believe this is happening, but also I can't believe it's a problem. And,

so, you know, a lot of times there's a technical issue in terms of the language in which documentation is often written, which is usually English; and there's another problem, a cultural problem, in making clear to some administrators that it really is an issue, at least in our culture, in our society.

MR. FRANCOIS: And that brings us to a good juncture to kind of talk about international aspects of open relays and open proxies, in terms of how much spam is sent through relays that have IP addresses of other countries.

MR. BROWER: In my experience, I mean, I don't want to tar any particular nation with the spam brush, but it's a moving target, as I'm sure others can attest. Brazil has come to the fore recently. And an interesting anecdote, recently in conversations with a Brazilian administrator, he found it annoying that the international language of the internet, by no one's design, I think, has become English. And he said to me, well, why can't we converse in Portuguese, and I had to say, well, because your English is noticeably better than my Portuguese. And then I said also, I mean, I'm not sure about this, but I imagine if you tried to land a plane is Sao Paulo and speak to the tower in Portuguese, you'll be turned back. That's just an unfortunate fact

of life, but it's one that can be remedied.

And I think one thing that we can address, and again, this is a nontechnical issue but a social engineering issue, one thing I think that everyone could address is to find methods to get documentation, including easy fixes, including deep documentation, available in many, many more languages than they are currently available in. That in itself would solve a lot of the problem, I think.

MR. FRANCOIS: I know that previously we had spoken about spam that you had received that had been sent through a relay in China.

MR. BROWER: Mm-hmm.

MR. FRANCOIS: And while you know a little bit of Mandarin.

MR. BROWER: Very, very little.

MR. FRANCOIS: I want to get you to discuss some of your experiences with trying to communicate.

MR. BROWER: Oh, well, I mean, I just -- I actually just -- again, I don't want to name names in a public forum, but, I mean, I will tell you that one particularly -- one point I made before, and I'll make it again. I again and again encountered administrators who said to me that it's an honor to be solicited for business. And I want to stress this as a socio-cultural

issue. It's not strictly and only a technical issue. I think we err when we approach it strictly as technical. In other words, is this proxy exploited, how do we get it closed? We need first to understand that the way in which we perceive the internet is not necessarily the way in which the rest of the world perceives it.

And, you know, I can -- are you referring to one particular -- you want to refresh my memory? Was there a particular anecdote we discussed, Renard?

MR. FRANCOIS: No, no, it was just something that I had scribbled down in my notes.

MR. BROWER: I wish you'd share it with me.

MR. FRANCOIS: Just talking about how difficult it was in terms of, first of all, the two barriers that you'd enumerated, the first was the barrier, the language barrier.

MR. BROWER: Mm-hmm.

MR. FRANCOIS: And trying to --

MR. BROWER: The socio-cultural one.

MR. FRANCOIS: Right. And then the second barrier being the socio-cultural area.

MR. BROWER: I can tell you this, that even -- I mean, interestingly enough, a couple of times I had in dealing with networks in China, I had to battle through to find the -- you know, the person whose English was

sufficiently superior to my Chinese that we could carry on in a rational conversation. And even at that point, many times I encountered that same cultural barrier, amazement that it was considered -- and by the way, we're talking -- also I should put it in context. This is a year and a half ago. There's obviously been significant education since then among many Chinese admins, due not in small part to the efforts of people like Steve Linford (phonetic) and Chinese admins all name Ed Yu (phonetic) as a good example of someone who's made a personal effort to educate administrators in mainland China. But, you know, some of the reactions I got were actually funny, but I don't want to really tar anyone.

MR. SERGEANT: Well, actually I can expand on that, as well.

MR. FRANCOIS: Excuse me, Matt?

MR. SERGEANT: I can expand on that, as well. That we've definitely seen a shift where we have kind of a unique perspective, being a global company, that we're seeing more and more customers in places like Korea coming to us and saying that actually we didn't believe spam was a problem but now it really is an issue, and we would like to stop it. So, there is some movement going on in those Asian nations to change their outlook.

MR. FRANCOIS: Go ahead, Dr. Hancock.

DR. HANCOCK: One of the things, we operate in 82 countries, and so we deal with this on a multi-national basis on a regular basis. I was at a forum in Japan just about a month ago, and one of the discussions there was how to cut down spam, and if it wasn't for the classic reason of spam is objectionable, it was because it was sucking up bandwidth. And as a result of that, that communication got through to the Japanese customers quite quickly, because someone is illegally using your bandwidth and illegally using your computers and taking away your resource, irrelevant of what it was. And that got their attention rather quickly.

When you tried a discussion with them on a social basis in terms of it's a security violation, it is objectionable content and all that, you have to remember that in other countries, such as Japan, child pornography is legal.

And, so, when you start dealing with different kinds of aspects of spam and what the content of the spam might be, in that country it might be a legal thing. But when you start addressing it as a someone's using your bandwidth, all of a sudden it became a very serious problem and the conversation changed quite radically. And, so, what you'll find is that I agree with the sociological issues, but I think one of the things you do

is you approach it as band width theft in those areas or space theft, and all of a sudden it becomes a very serious ordeal when you start dealing with folks in the other countries.

MR. FRANCOIS: And, Adam, I wanted to kind of -- and maybe this is a question for all of you who have dealt with the problem of international open relays, is to ask once you get past the first and the second obstacles, the language barrier and the social barrier, do you find that the system admins are particularly helpful and willing to resolve the issue?

MR. BROWER: I would say anxious to. You know, once they're apprised of the actual problem, but again, there still is the barrier of language in the documentation, and I think that's a serious shortcoming and one that we have not addressed as, for want of a better phrase, as a community. I'm not sure we are one, but as a nascent community, I think that's something we could address. Making, you know, world lingo and babblefish and other on-line translation services are notoriously hilarious in their renderings of technical language particularly.

And, so, you know, I think in line with what Bill said, making the point that theft is frowned upon in every society, I guess is a good way to boil that down.

And then having documentation that makes it very clear to admins how to fix security holes in their software in their own language will facilitate that. So, I really think that the availability of documentation in various languages is a very important issue and needs to be addressed.

MR. FRANCOIS: There are two follow-up questions that I wanted to ask about international open relays and proxies. The first would be out of the 400,000 -- or approximately 400,000 open relays that Nick told us about, is there any way to quantify how many of those are international?

MR. NICHOLAS: My guess is it's the majority of them are. And that's just derived from my experience in studying the issue over the years. I can't quantify it any further than that. But they particularly seem to be in the lesser developed countries, where the level of education is not quite as great as it is; the sensitivity to the issues is not quite as great as it is in the States. But certainly the United States is not immune either.

MR. FRANCOIS: And also in terms of open proxies, is there any way -- is that an international problem, as well, or is it mostly domestic? Michael?

MR. RATHBUN: Well, the problem is being dealt

with, but there was a time when the standard issue system that was put into Korean public schools was a software load that included an open mail server and an open proxy. And that was a bonanza, to the point where there was, in fact, a DNS-based advisory list that would specifically tell you, yes, this IP is in Korea. And, again, this is something that the Koreans themselves have been grappling with, and I know we'll hear more about this later on in the forum.

But it highlights a particular kind of genesis of this problem from my perspective, which we touched on to some degree earlier, in that in many cases what we have is something that was built to be insecure, either because in the case of some of these software loads they were put together when open proxies and open relays were not customarily abused or there is just resistance to what I would call a product quality and a safety and suitability issue.

MR. FRANCOIS: Actually, I lied, I still have two more follow-up questions on this. The first is we'd heard on a previous panel that a panelist said that Spammers were paying open relay or operator systems administrators to maintain open relays internationally. And I'm just wondering, is that your experience? Is there anecdotal evidence that you found about that, that

people are actually in the United States giving money to people internationally to keep an open relay?

MR. BROWER: I can speak to that anecdotally, and again, without naming names, I should say that it's part of my practice as an independent consultant I often have to deal with what in military terms would be termed dark sources. But I had occasion once to speak to an administrator in Romania and was told shortly before he cut the wire that he had been given a certain honorarium, and again, I hate to use the name -- the word certain, by a certain American, relatively well known entrepreneur, let's just say. And when I informed him that I was going to forthwith deny those IP addresses to the deny tables to which I had access and that I would recommend others do the same, he I guess had further negotiations with the American entrepreneur and sacrificed the remainder of his honorarium. So, yes, in short, I have personal anecdotal evidence that it is possible to bribe someone to keep a relay open, sure.

MR. FRANCOIS: Dr. Hancock, you look like you were shaking your head down there.

DR. HANCOCK: Well, I've seen both extremes, but to be frank about it, the bulk of the folks that we run into, because we have embarked on scanning our network, and you're talking about 3 million IP addresses

just in Asia alone. When we contact the customers, by and large in Asia and in Europe, the customers are shocked that they are able to be used. We have run into very, very few that are actually being paid to keep the relays open or to keep a proxy open.

Now, the bulk of the situation that we've run into with proxies is that a lot of proxies that were originally developed were part of like firewall tool kit and things like that, and those proxies out there were for generic purposes so that you could use other protocols through it, as well. As a result, those technologies are still there, and they are used for other protocols like Tuxedo and what have you like that, and they make a very nice place to go back and relay e-mail through, as well.

So, what you find out very quickly is that a lot of people have these things open because they were there all along or they need it for another protocol. But what you'll find also is that they don't necessarily keep them open because they're being paid for it. Now, I don't disagree that there are some cases where that is the case, but by and large what we've run into with our customers is they're usually shocked that they're involved in something like that and they didn't know that it was open to start with, or they had it open for a

specific reason that had nothing to do with e-mail.

MR. BROWER: Yeah, I certainly didn't mean to imply that it was an endemic problem, but only that in fact it does happen.

MR. FRANCOIS: And the final question, before we kind of close out this issue, is just a question from my perspective is it is easy to tell, and if it is, how much spam is actually generated in this country but relayed internationally back to this country?

MR. NICHOLAS: Yes, it is easy to tell. That much you can generate help from headers, and there is quite a bit of that going on. What appears to be international spam originating from Chinese servers actually originated in the United States. We know this because the spam itself is in English. They are promoting American-based companies and American-based websites.

MR. FRANCOIS: Anyone else?

Okay, so moving on to -- Matt and Nick briefly talked about kind of resolving the situation with relays and proxies and talked about patching or reconfiguring their systems. And my general question is for open relays -- for both relays and proxies how easy or difficult is it to reconfigure the system for the intended user or the person that is most likely to be the

one that has installed the relay or proxy, whether it's a systems administrator or a person at home trying to create their own network? And also in addition to how easy it may or may not be, is it very expensive to do?

MR. NICHOLAS: I can speak on it to the proxies issue, and I'll let -- I'm sorry, relay issue; I'll let Matt deal with the proxy issue. It's actually very simple in most cases to lock down a server that is unsecure. Often it's just a matter of a single configuration line in a configuration file. The problem is knowing which line it is that needs to be locked down, so there is some amount of education that's required in order to do this, but I would say by and large the time and effort is relatively minimal.

MR. FRANCOIS: Now, in terms of the education, do they find that on a website? Do they get a contractor?

MR. NICHOLAS: MAPS sponsors something called the transport security initiative, and the whole purpose of this project was to make the information needed to secure various programs, whether it be sendmail, queue-mail, post-fits, et cetera, it would tell you exactly what you needed to do to go in and lock down that server.

MR. FRANCOIS: Okay. Matt?

MR. SERGEANT: As far as open proxies go, it

changes slightly more, because there seem to be more pieces of software for running open proxies than there are for running SMTP servers. But in general, the most common piece of software we seem to see is Analog X, and changing its configuration is a matter of opening the preferences dialog, entering an IP address, clicking OK and then it's done.

MR. FRANCOIS: Anybody else? How big -- in terms of the amount of spam that we are probably going to discuss on Thursday and Friday being problematic and the enormous costs that imposes on businesses, ISPs and consumers? And I know it's speculation, but how much of that do you think is attributable to spam sent through open relays and open proxies?

MR. RATHBUN: Again, what I've noticed on Earthlink's network is that 40 to 50 percent of the spam sent to our network or really through our network is due to misconfigured proxy servers or open relays, at least.

MR. FRANCOIS: And of the 40 percent of the spam that you all get through open relays or proxies, as a percentage, how much do you think that you all are able to find, process and take action upon, whether it's contacting the relay operator or server owner and taking -- advising them to take steps to close the relay or secure the proxy?

MR. RATHBUN: With mail sent to our network that did not come or was not relayed through it, we will send off reports to the originating networks or the networks where the mail was relayed through, so I can't speak to how many of those issues get resolved, but for our own -- on our own network, a good portion of my day is spent calling customers with these problems and making sure that they all get secured.

I'd say if -- out of the percentage of mail that was sent from our network through using these insecurities, close to 100 percent of them, as long as they get reported to us, get resolved; or we will resolve them on our own.

MR. FRANCOIS: And how will you do that?

MR. RATHBUN: We may have to shut down service for a time, but normally that's when we'll get a quick call from the customer.

MR. FRANCOIS: So, we've talked about kind of the open relays, proxies problem; talked about a cost-effective way to try and remedy those situations, and I'm going to turn to Brad to talk about another potential solution that you can use for probably a couple of ways, and that's honeypots and what they are and what they do and what you do with them.

MR. PATTON: Honeypots are computers that are

connected to the internet and are designed to look like an ordinary or insecure, in this case, mail server or open proxy. They can be used as a tool to detect illicit activity on that computer. From that information, we can detect trends or specific problem IPs where we are getting scans to the honeypot, scanning for an open relay or an open proxy server. So, it can be a useful tool if used correctly.

MR. FRANCOIS: What types of information do you all -- does the honeypot get from people who are trying to manipulate the system?

MR. PATTON: It would show you who was logged in and from where, if you could find out where that IP was located. Basically you can detect trends to see if a lot of people are scanning for a certain type of insecurity or if it's coming from a certain region, and perhaps you can take measures to filter some of the traffic coming to your network from that area.

MR. FRANCOIS: What region do you find mostly is trying to get into the Earthlink system?

MR. PATTON: I wouldn't know any specific region where they were coming from.

MR. FRANCOIS: Okay. The other thing that -- have you all used from the information, and you may not know about this, and other panelists may, but have you

used information that you've gathered in using honeypots to litigate against Spammers?

MR. PATTON: Not to my knowledge.

MR. FRANCOIS: Okay. And do you know roughly how much on a daily basis maybe you acquire the information, process it and maybe block a particular IP address based on what you find in those?

MR. PATTON: I wouldn't know any specifics with that. We use what you would call spam-trap addresses more than honeypots. A spam-trap address is what a honeypot is to a server, a spam-trap address is to all e-mail addresses. It's an address that is basically a dummy account where no one signs up for any e-mail lists, no spam or anything like that, and after a time, spam will be sent to that address, and you know that anything sent to that address, because it's never been signed up for any list, is obviously unsolicited e-mail. And, again, you could use it the same way as you would a honeypot, try and see where this mail is coming from, if you can block the sender from sending more mail to your network, because again, you know it's spam right away if anything gets sent there.

MR. BROWER: Could I interject something here?

MR. FRANCOIS: Yeah, sure.

MR. BROWER: I heard a tale of a woman named

Nadine.

(Laughter).

MR. BROWER: I wonder how many of you are acquainted with Nadine.

MR. FRANCOIS: If you can do it briefly, you might want to go ahead and explain.

MR. BROWER: Well, I think I may defer to Mike on this.

MR. RATHBUN: I'll tell you that Nadine is getting an increasing number of pieces of e-mail every day that are relayed through open relays and open proxies, and the last time I did an analysis of the Nadine traffic, in fact, the trend was toward an open proxy feeding an open relay.

For those who don't know, I operate a small domain that at one time accepted mail addressed to anything, and a woman in the southern United States signed up for a sweepstakes one day and gave an address that was on my domain. I had never met the lady and haven't yet, but since that time in the year 2000, her address has propagated all over the place and fallen into the hands of the most amazing variety of mailers.

Given that she actually failed to exist, it could be argued that she failed to opt in to any of these things. So, Nadine is kind of a special case spam-trap

address, because it was basically an address that was acquired by a major mainstream reasonably legitimate mailer with the belief on their part that it was actually given to them with the permission of the actual account owner. It wasn't, so that's really pointing out part of the security issue. But it escaped from the realm of more or less legitimate respectable mailers out into what I call the world of the gutter Spammer approximately nine months. And now it's quite a menagerie.

MR. BROWER: Mike, what's the current volume of Nadine's accumulated message load? Do you have an estimate?

MR. RATHBUN: Well, it's difficult to say, because as things stand now, I let any given mailer have three shots, and then I block them.

MR. BROWER: You would have run out of disk space theoretically by now --

MR. RATHBUN: Right.

MR. FRANCOIS: One thing I want to turn to you, we've talked about proxies, relays and honeypots and potential solutions. I want to talk to -- and we've heard Michael Rathbun eloquently describe the escalation that goes on or that has gone on from a dial-up account to the ISP response to the Spammer response to that by going to relays, the response to that by -- and then the

Spammer responds by going to open proxies and it just seems like for every action there is a reaction from the Spammers. And, so, part of -- the last part of this panel is going to talk about the future of spam and the exploitation of security weaknesses that have started. And we're going to turn to some issues that have come up in the last six weeks and I'm going to start off with Adam Brower on that, and we will then talk about -- and then we will move to a closing presentation from Dr. Bill Hancock. And, so, we've got about 11 minutes.

MR. BROWER: Okay, I'm going to try and talk very fast. No, no, I'm only -- I'll talk slowly.

MR. FRANCOIS: Well, we're going to save time for some questions, so that's more.

MR. BROWER: I'll still try to talk fast or quickly and properly. I wanted to raise and issue that was raised at the first panel today, and that is the issue of zombie or legacy blocks, which seems to be the flavor of the month. And I've been involved in a couple of interesting BGP shenanigans recently, trying to chase down the perpetrators of them. Briefly, for those of you who don't, you know, aren't up on this or aren't aware of it, I can -- being myself a layman, I can probably describe some of it in layman's terms.

A company, Xco, has a domain, xco.com, and they

wind up getting a block of IP addresses. And in the fullness of time, xco.com goes out of business. And for whatever reason, be it good bookkeeping or just anxious to get down to the Bahamas and play with their boats, they don't -- there's no traffic issuing from that block of IP addresses. It's just sitting there; it's not used; it's not announced anywhere even. And by announced I mean it's not propagated to all the other computers; it's not visible to the internet at large.

So, along comes an enterprising -- again I have to use the term entrepreneur, who says to himself, well, how hard would it be for me to make a piece of letterhead, representing myself as xco.com. People at ARIN may not be aware that xco.com is out of business. And lo and behold, that works. What happens is that zco.com winds up controlling xco.com, and then they contact the backbone and say we're in control of this block and we would like you to announce it. And lo and behold, backbone X announces it.

This is very much social engineering, in the classic sense of the term. And a lot of it's done by telephone and fax. I really am Bill Jones of xco.com, and honestly, you know, we just want you to announce this block for us. I've seen it happen, and inevitably, of course, or maybe it's obviously inevitably what the

material that the websites wind up hosting those IPs is bogus in every sense of the word.

Now, as it works out now, there's kind of an unofficial -- I won't say cabal -- I'll say group of people who gather in various media to discuss these issues, typically in tones of outrage, how could it be that so-and-so is announcing such-and-such a block? And then what generally happens is somebody gets on the phone to somebody they know, all unofficially now, in outsider channels, and that route is scrubbed.

What a friend of mine proposed, and actually a relatively erudite internet consultant, someone I really respect on these issues, proposed, and this is just a starting point for discussion, an international clearing house of inactive blocks, which when requested to announce or activate a block, Backbone could consult, you know, so it wouldn't -- you know, having a block in that clearing house would not necessarily mean that it was about to be hijacked for Spamming, but the fact that it was in that inactive clearing house would mean that the Backbone or the provider would maybe do a little bit more diligence in investigating the bona fides of the person applying to have the route announced.

And that's a starting point for discussion, and I'm sure other people may take it up or they may think

it's a bad idea, but that's the idea we came up with.

MR. FRANCOIS: How prevalent has this problem become?

MR. BROWER: More and more so. In fact, there are probably lots of legacy or zombie blocks out there right now that are undiscovered, just because frankly it's very tedious investigative work that's required and it's often not the sort of investigative work that technically skilled people are adept at, you know? It's not all about octets and stuff like that; it's about forged letterheads and what somebody's real phone number is. So, it's actually more forensic detective work, honestly, than IP-based stuff.

MR. FRANCOIS: So, once someone has control of this block, just how many IP addresses do they now control?

MR. BROWER: Well, what is the exact number in a slash-16, Michael?

MR. RATHBUN: 65,000-some-odd.

MR. BROWER: A large number.

MR. FRANCOIS: And with the approximately 65,000 IP addresses that they have in that block, generally how much -- what damage can they do from a Spamming point of view? How much spam can be sent before it gets shut off?

MR. BROWER: Once you have that resource, there's any number of things you can do. You can host -- spam-vertise -- you may advertise --

MR. FRANCOIS: Speak into the mike, please.

MR. BROWER: You may -- ooh, that was too close. You may spam-vertise a given domain from outside of your hijacked network and then of course find that it's virtually impossible to have that advertised site taken down because you control the slash-16. That's one obvious use. And it also, by the way, there are other obvious giveaways here, and typically you'll have an ASN that you control a slash-16, you have an ASN, you're only announcing 1/24. That kind of makes you curious, you know, as an administrator.

I mean, so the point is that once these problems come up they're not hard to find, but if your question is how valuable is that resource, immeasurably valuable. I mean, it gives the Spammer basically control of his own network. And there's no upstream in many ways.

MR. FRANCOIS: So, short of this repository of deactivated IP addresses or blocks, what are some short-term interim steps that can be taken to kind of guard against this and who needs to take those steps?

MR. BROWER: This particular problem, I think

the largest issue that needs to be addressed, and this is an issue of personnel and income, frankly. As we know, providers, as an industry, many of them are severely squeezed for money right now. They've been involved in a race to the bottom, competing only on price for so long, that many of them are operating on razor-thin margins.

And as a result, they cut in terms of doing diligence, investigating prospective customers, doing checks on addresses, things of that nature. So, you know, I hate to say this, but raise prices, from a practical standpoint, and compete on quality, rather than price. And I've been making this case for a long time, and of course it's very easy for me to say, you know, I don't control a corporation that's running on one-cent margins.

But it seems to me doing diligence, actively investigating, to the best of your ability and with available resources prospective customers in every respect is very important.

MR. FRANCOIS: Thanks.

MR. BROWER: You're welcome.

MR. FRANCOIS: Now I'm going to Dr. Hancock, Dr. William Hancock from Cable & Wireless, who is going to give us a glimpse into the future of some of the techniques and what's coming down the pike for spam. And

security weaknesses.

DR. HANCOCK: Thank you, Renard. That's like calling Godzilla a lizard, so we'll see how it goes from there.

In the past, we have the internet, this is a picture of it in 1988. Back then, mail relays and different types of mechanisms to move things around, the biggest spam you had was the announcement of a seminar at Bell Labs or something like that. And this is a current picture of the internet today.

(Laughter).

DR. HANCOCK: This is actually off the Bell Labs' website, and this is a picture of only the United States. And one of the little endpoints of those little lines over there could easily be a mail server. This one here I'm bringing up for a point that I'm going to make here in a minute. What you see at the very bottom bar is Windows 3.1; the very last bar over there is Windows XP. Windows 3.1, approximately three million lines of code; Windows XP, approximately 45 million lines of code.

There's a known statistic in software engineering that states that basically there are ten bugs for every thousand lines of code. And it's probably much worse than that, but that kind of gives you an idea to think about, because one of the ways that we're going to

see spam spread in the future is the exploitation of bugs on an operating environment.

Let me give you a very brief example of that. On January 25th, the internet was hit with something called slammer. Slammer basically took advantage of an exploit on ports 1434 and 1433 of the UDP protocol based upon a bug in the Microsoft sequel server. That bug was fixed approximately seven months earlier; there was a patch available. Since that time, approximately 450,000 servers were exploited with that particular whole in that bug. The slammer worm that propagated around the internet had a payload that did nothing, but it did gain complete access to the machine. That payload could easily have deposited a mail relay server, very easily.

So, what you're seeing in that situation with the slammer worm on January 25th, was that it was a band width consumption attack using a bug, a single bug, on a particular product, on a particular Windows platform. That was actually fixed, but people didn't put the patch in.

What's important about that is that Spammers are already starting to create tools to exploit these kinds of things, where they can actually send to you a mail relay server, even if you're not running one. And the result of that is tools like worms like slammer allow

the opportunity to go back and take advantage of bugs in very large and very complex operating environments such as Windows XP, Linux Server, so on and so forth.

So, it's important to understand that as long as we have complex environments we have complex software, we continue to have buggy software. We have the opportunity for infiltration into the machines, and as long as that exists, when you start using things like worms and trojan horses to transmit the data, the opportunity to infiltrate the machine and deposit malware is very, very good.

Everybody happy yet?

(Laughter).

DR. HANCOCK: This little statistic over here is from CertCC that basically shows that between 1998 and 2002 the number of attacks jumped from approximately 1,928 attacks to well over 86,000 attacks in 2002 alone. Now, these are the documented attacks, and it's estimated that this is only 3 percent of all the attacks you see on the internet.

More importantly, these are the number of vulnerabilities that have appeared, just in a single year, and the vulnerabilities are ways that you would use to infiltrate an operating system and application or a system to deposit malware, whatever that may be. And it

could be something as simple as a password grabber, or it could very easily be a mail relay system.

Now, I particularly like this particular chart. This is one that Rich Pethia (phonetic) puts up from CERT. And what you see in the bottom left-hand corner is starting approximately 1988, going all the way up to 2002, the sophistication of a security attack on a computer system. So, as you see over time, the attacks get more and more sophisticated, and frankly, they have to, because the operating environments, the applications and everything else are getting more and more complex. That dotted line that you see, going from the top left-hand corner, going down to the lower right-hand corner, is the intellect of the attacker.

(Laughter).

DR. HANCOCK: So what you're seeing is very sophisticated attacks being launched by morons, okay?

(Laughter).

DR. HANCOCK: And, frankly, I've got statistics to back that up.

(Laughter).

DR. HANCOCK: We find that on our networks and all that we operate a very, very large multinational network. We find that the bulk of our attacks happen between 4:00 on Friday evening and 9:00 on Sunday. And

80 percent of them are launched by kids, because most of them don't have a date and don't know what to do that weekend.

The bottom line is, though, that it means that those people are able to download very sophisticated tools from the internet, use those sophisticated tools to launch zombie networks to go back over and infiltrate other machines without themselves having the intellect to know what they're doing. In fact, I've been involved in over 600 prosecutions and I can tell you categorically every time we run into a kid they have no clue what they're running. Very rarely do they understand the tool that they downloaded and what that tool actually does. And as a result of that, spamming somebody is becoming easier and easier.

We were recently involved in a situation where there was some spam going on, and it was a bunch of teenagers who had downloaded tools and were Spamming other people in their school. And they were doing it for money, and the result of that meant that they didn't know what they were doing. All they knew was that they ran the tools a certain way, provided the spam in a certain way, the next thing you know, they made money out of it. And, you know, there are ways for other people to get their allowance, but this one worked rather well for

them.

So, what's the entry point cost of making spam? Basically a PC, some software you can download and a network connection of some sort. It doesn't take a lot of money to become a Spammer. It does not take a lot of money for someone to get into the business. This makes it a very low entry point. One of the big things about cyberwar, if you ever study cyberwar concepts is that cyberwar basically says it's non-lethal warfare. You don't kill people, but you can make their life very miserable from an economic perspective. You can disrupt all kinds of economic factors involving a company, involving an individual.

What's important about this particular thing is that it doesn't cost much to get into the spam business, and yet you can generate fairly good revenue. This means as long as that matrix exists, you can legislate it all day, you can try to put in technology all day, but as long as the money keeps flowing, someone's going to figure a way around it.

The core span need of course is to make a server out there for you. Basically right now people use servers that are in existence that someone has brought up, either accidentally or intentionally, whatever the case may be. But the bottom line is that you're looking

for a server, you're harvesting addresses, you're going to use those servers either as an open proxy, open relay or in some cases a direct connection, if you're using different types of protective IP addresses, or if you go back and scan IP addresses. But in all cases, you have to have a server to make it go out the door.

The biggest thing also that Spammers have to do, they have to evade capture. That's one thing to sit down and say gee, we'd like to go back and spam, but you have to be able to evade being caught and evade that your server, when it is caught, you can go someplace else and be able to go back and spam. Because of that, you have to be agile and you have to be mobile. And that means that the need to move around is a very critical part of becoming an effective spammer in the future.

Now, this brings up the upcoming methods. One of the methods we starting seeing very recently is of course the ability to use what is called a trojan, if you will, a trojan horse type of application, which comes in, basically attacks a system, and then launches itself inside the system, providing a server capability. That's one way. And this can be done through a variety of methods. There's ways to do it via hacking, you can just go back and hack it, use a known back door, use a known hole like the slammer did, and then deposit the server

capability into that machine.

Now, what that translates to is that everybody who has a machine that's connected to the internet and according to the Internet Society as of last month, there are 655 million user accounts. That means that anyone with a PC out there, even if they're not running e-mail whatsoever, could be attacked, could have a server imbedded on their machine, against their will, and then that server used as a spam relay site.

And, in fact, there's at least four programs running around the internet that do exactly that. And that means that you don't have to use an open relay, you don't have to go back and use an open proxy, you yourself are depositing that e-mail server as part of a package when you go back and bust their machine.

As a result of that, you can set up what's called spam distribution networks, very similar to what denial-of-service-attack people do with zombie attacks. Most of you folks have probably heard about denial-of-service attack. How many of you have children? How many times you go into the potty and you find that it's full of toilet paper and a plastic truck?

(Laughter).

DR. HANCOCK: That is a denial-of-service attack.

(Laughter).

DR. HANCOCK: A distributed denial-of-service attack happens when they bring 12 of their friends over.

(Laughter).

DR. HANCOCK: So, it is not a very sophisticated attack, it doesn't take a lot of logic to do it, it doesn't take a lot of intellect and it's not that hard to do because it sucks up bandwidth. If you suck up the bandwidth, there is no way that anybody can get to what you're after. In the case of spam, by using the same distribution methods that are used right now to distribute zombies or basically small pieces of code that go all over the network, you can now go back over and distribute these trojans and basically provide an SMTP service capability on unsuspecting machines.

So, a lot of people want to say, oh, okay, well, how does it work. Well, basically the first thing you do, somebody sits down there and they create the trojan horse program. And then they also go back over and create a worm. Okay? Now, when the worm comes up, the worm basically has a payload in it and it has some methodology of replicating itself.

Well, let's understand what that means. Code red, when it came out in 2001, basically took approximately 37 hours to replicate itself around the

internet. The slammer worm in January of this year took eight minutes. Everyone get that? Thirty-seven hours to eight minutes in less than a year and a half. That's important, because it means that the propagation capability of a malicious worm that contains something that will go back over and infect networking resources is very, very easy to do with current technology and current science.

Now, once these zombies are all out there and they're all positioned, they're ready to go, then the person who operates the spam at that point goes back over and creates the evil e-mail. And then at that point they can distribute the evil e-mail of course over to the network that's out there. The network at that point then goes back over and attacks the poor, hapless end-user, who ends up getting their mailbox full. And this is the sort of thing that happens and all of this is known science. It is not that difficult to do.

So, as we look at issues with this sort of approach, basically what you've got to have is automated distribution. We call this AML for autonomous malicious logic. The purpose of this is basically using the same techniques that are used for denial-of-service attacks to go back and distribute zombie networks, now you're distributing AML-oriented SMTP networks that can then be

called upon, they can be shared. You can distribute thousands of these in an hour. It doesn't take very long for this sort of thing to get out there, because people do not adequately patch their systems because the systems have a great deal of code, because they have bugs, because there's all kinds of ways to infiltrate and infestate the systems.

Legislation is not a problem, because when we've legislated all day long, they just go off shore. A good example of that is viruses. How many legislative things have we seen attended to viruses and how many has it stopped? Every month there's approximately 250 new viruses that appear. It's a billions and billions of dollar business. As a result of that, there is a money flow; there are reasons for viruses to be created. I also find it very interesting that many times new viruses seem to appear towards the end of a sales quarter, but that's a different issue.

(Laughter).

DR. HANCOCK: Go back and look at it yourself. And in the situation, as we can go back and legislate it, but what happens is when we pass legislation in the United States against spam, we're going to turn right around and see it getting broadcast and being taken care of internationally. A lot of links in third-world

countries and folks that are just coming around to the internet and very, very large organizations and things like China, they don't have protective capabilities, they don't have ways to go back and stop this and they may not know how. You start parking a zombie network in those types of environments, and the spam situation internationally gets worse, and legislation is not going to stop it.

Problems that we're going to have to think about the next five years is that most of us are going to go mobile. If you're not mobile already, you're going to get there. And that's through 3G cell phones, through Wy-Fy hot spots. There's all kinds of wireless technology. Saying that we're not going to have spam problems in these types of technologies is ridiculous, because we're already starting to get them now, okay?

What's going to happen in the future is that your personal cellular device, your cellular device will also be connected to things like Wy-Fy telephones. As a matter of fact, Cisco announced one yesterday -- the day before yesterday, I believe. And you're going to find these kinds of technologies out there where the phone becomes your local area network connectivity appliance with an IP address and simultaneously can be your cell phone when you get out into the world running around.

That means that that device has an IP address. You can actually download to these things, because they run in microkernel, unix, linux or microkernel Windows environment, a very small e-mail relay. So, you may very well find that your phone is getting very fat in your pocket because it's filling up with e-mail because it's relaying it out to other phones in the area.

So, why do we need spam protection? I always put this up as my favorite little picture. That's because it's my 13-year-old. This picture was taken on Sunday. That's his cat.

(Laughter).

DR. HANCOCK: In reality, that's a full-grown Bengal tiger named Savannah that lives down the street, so he plays with her off and on. Notice the satisfied look on her face from eating the previous Spammer.

(Laughter).

DR. HANCOCK: And the point being is very simple, is that my son at age six has grown up with a proper geeky lifestyle. In fact, when he was born, they handed him to me and I said welcome to the world, my son, I'm your father, and COBAL sucks.

(Laughter).

DR. HANCOCK: And I have this on videotape. I actually did that.

(Laughter).

DR. HANCOCK: My son has grown up very, very good in the geeky lifestyle. He has the proper 2.3 computers in his bedroom, and of course with a T3 connected in the house, my son is well equipped to go back and deal with internet capability. It helps to work for a carrier.

(Laughter).

DR. HANCOCK: The situation is, folks, is that my son also came in at the ripe age of six and said, Daddy, what is a penis? And I said why? And he said someone sent me an e-mail where I can make mine bigger, and I thought great, this is what I need to hear right now.

(Laughter).

DR. HANCOCK: Although lately he's been asking about breasts and it bothers me a bit. The situation is that these kids get this stuff. They get it at school; they get it in high school; they get it all over the place. Well, to adults, it's somewhat of an irritant; to kids, it really sociologically causes them some very serious problems. And, so my major reason why I am very much anti-spam and why I spend a great deal of my time worrying about it, stopping it, scanning for it and finding it and killing it dead, is because of my son who

likes to hug a tiger. Thank you very much.

(Applause).

MR. FRANCOIS: Thank you, Dr. Hancock. We are going to take questions from the audience now.

MR. HUSEMAN: Well, we have one quick written question.

MR. FRANCOIS: Okay.

MR. HUSEMAN: The panelist mentioned the numbers 402,000 for the number of new open relays and open proxies per day, are those new open relays per day or newly discovered open relays?

MR. SERGEANT: Newly discovered.

MR. HUSEMAN: Newly discovered, so they were already existing? Okay, thank you.

MR. FRANCOIS: How about over there? Yes?

UNIDENTIFIED SPEAKER: Too many questions to ask and not enough time.

MR. FRANCOIS: How about pick one? The shortest one.

UNIDENTIFIED SPEAKER: In speaking of honeypots and receded e-mail addresses, we've done that many, many times and we never could figure out how they found that address. Is that like from dictionary Spamming? Also there's been a sudden and very steep increase in the amount of spams that come that are like numbers separated

by equal marks. There's no text in the spam at all. There's no subject line or anything. It's all just characters separated by equal marks, and someone told us this was an e-mail to find out if our mail server was compromisable or had been compromised. Can anybody speak to that?

MR. FRANCOIS: Mr. Rathbun.

MR. RATHBUN: Well, some of the ones that you get with what would sound like to be encoded probably Asian language sets, I get probably 45 to 50 spams a day that are in Chinese or Russian and they look that way.

MR. SERGEANT: Yeah, that sounds like quoted printable.

AUDIENCE MEMBER: Quoted printable.

MR. FRANCOIS: Other questions? Anybody? Okay.

AUDIENCE MEMBER: Thank you. We know that data has overtaken voice over normal telephone lines. Do we have any statistics on how many e-mails per day are actually being sent, either in the U.S. or worldwide?

MR. SERGEANT: It's about -- for our corporate customers, it's around about 40 e-mails per day, per user.

MR. FRANCOIS: Let's go -- any questions -- right here, in the middle. Hang on, and let's get you a

microphone. And give me time to repeat part of the question, as well.

MR. IVERSON: I'm Al Iverson (phonetic) from Digital River. I actually used to work for MAPS and open relays are something that I'm pretty familiar with. One thing I'm kind of wondering, any of you folks, especially from a provider perspective, do you run into any open relay operators that absolutely defend their right to run an open relay and won't do anything about it? Obviously Michael knows I'm thinking of somebody named John Gilmore --

(Laughter).

MR. IVERSON: -- who I've come to realize that was somebody we ran into where he wanted to sue everybody who wanted to block spam from that relay.

MR. FRANCOIS: The question is from a provider perspective have they run into anyone who operates an open relay that defends their right to run an open relay.

MR. BROWER: Well, I have run into maybe one or two people over the course of working at Earthlink that have felt that way, but we have a policy to uphold, we can't allow spam on the network and unfortunately, we just can't allow it. I don't really understand why someone would be so adamant in keeping their relay open.

MR. FRANCOIS: And what were some of the --

briefly some of the arguments that they used to justify keeping it open?

MR. BROWER: The one I can remember would be -- it was just kind of silly. They did not feel like they should have to change it. They had it set up from the box the way the actual software was set up, it was open for relay when they installed it, and he didn't feel like he should have to change it.

MR. FRANCOIS: Michael, it sounded like you wanted to say something.

MR. RATHBUN: From the standpoint of shall we say a doctrinal or a philosophical stance, we don't really see that too much. Mostly it's either just planting your hooves because you don't feel like somebody else should tell you how to run your system, or the one I heard most recently was that nobody had the guts to go and tell the CEO that he had to reconfigure his laptop.

(Laughter).

MR. FRANCOIS: Any other questions? Way, way back in the back.

AUDIENCE MEMBER: Can you hear me? Can you hear me now?

(Laughter).

AUDIENCE MEMBER (Partially audible): -- Double Click. This kind of goes to the open proxy question. I

think by now we've all heard some variation of this story, I was in a hotel or I was in Starbuck's and I just turned on my computer and my wireless card and boom, I'm on the net. And that's been my experience, too, for $3 or $4 -- we've all heard about the Pringles can -- (inaudible) -- wireless card that pick up connectivity three miles away. And I tried the experiment from my house, you know, I was easily hypothetically on five or six people's networks without much work. Now, what kind of a threat does this pose, if I was -- (inaudible) -- Linux box with an MDA built in, you know, is this a real threat and are we finding that kind of connectivity to be Spammer's next choice?

MR. FRANCOIS: The question is what kind of a threat is wireless connectivity and is this the next Spammer choice? Takers?

DR. HANCOCK: It's a huge problem already. We've got an awful lot of wireless capabilities running around within the company called Cable & Wireless for a reason I guess. One of the situations I keep running into is that even our own folks put up wireless networks and sometimes inadvertently leave something open and someone wanders by in a car or driving or some nonsense like that and they're on.

The biggest problem that we're seeing right

now, though, is that with the predominance going to wireless and especially 802.11A, and 802.16, which just announced two months ago. 802.16 is a metropolitan area wireless which allows you anywhere from 54 megabytes up to 100 megabits, and allows it over a 30-mile range, and so, therefore, the limited range of 82.11 of 825 feet is about to go out the window. And with that kind of capability, you now have a metropolitan wireless capability that anybody can tie into. And that means that you don't have to have wire; you can obviate the local loop; there's all kinds of ways to easily connect to this. And the base security at level two at these things to connect in and authenticate is a joke.

As a result of that, it's very easy to connect to these kinds of networks and use them for legitimate connectivity with an IP address and become a relay of any kind. So, if you add that into the capability of also assigning zombie code and things like that to these kinds of machines, it's going to be a very large problem. We've already got the problem now of just people illegally using those kinds of networks, using them in an illicit way as well is going to be a real problem.

MR. FRANCOIS: One last question. Anybody? A hand back there.

MR. SOUDER: Hi, Doug Souder, from Hunting

Software. In the session where we were talking about harvesting e-mail, somebody said that that was the air that keeps Spammers going, and I was just wondering if we could somehow get the upper hand on the open relays and the proxies. Do you think it would have a similar impact? Is this the air sustains these Spammers?

MR. FRANCOIS: The question is how can we get the upper hand on open relays and open proxies and is this the air that sustains the Spammers? A very short answer.

MR. BROWER: I have a very short answer.

MR. FRANCOIS: We'll take it from two, Adam and Matt.

MR. BROWER: I hope mine is shorter, and the only time I'll ever say that.

(Laughter).

MR. BROWER: I've been reading too much spam. I think the technology is the answer and sociology is not the answer. So, I mean, and I'll take this opportunity to be entirely off topic for this panel. I believe firmly in DNS-based IP blocking, combined with rigorous white listing as the only solution to this problem.

Now, there are ways to get around it, but as far as I can see, going forward, that's the only thing that will work.

MR. FRANCOIS: Matt?

MR. SERGEANT: It's an arms race. We will -- you know, we will beat the open proxies problem into submission, hopefully, and there will become other ways, as Bill has described, that they will find other ways of distributing their stuff.

MR. FRANCOIS: One quick question from me for a yes or no answer from the panelists. Basically, should the government in terms of -- we talked about companies scanning their proxies and servers. Should the government also get involved in scanning for open proxies and open relays? Yes or no.

MR. SERGEANT: No.

UNIDENTIFIED SPEAKER: Waste of time.

MR. FRANCOIS: So, we've got a no, no, a waste of time and?

UNIDENTIFIED SPEAKER: No. In case you didn't hear me.

MR. FRANCOIS: All right, so everybody agrees now, and I wish we would have had more time to go into the reasons why, but we are at the end, and I have a few announcements that I need to make for the end of the panel.

First, on May 16th, the Federal Trade Commission and its Southwest partners in the Netforce are

going to make an announcement and have a press event in Dallas, Texas concerning open relays, so please stay tuned.

Administrative announcements, today is the end of day one, and we want to thank you all for braving the cold temperatures, the bright lights and the long lines.

(Applause).

MR. FRANCOIS: It's been a very productive day, and I just want to make three quick announcements. One, as always, it's about your name tags. Panelists, hang on to your name tags if you're going to be back for the duration or tomorrow or any day. If you have one of these peeling name tags, then you will have to get another one tomorrow. The one you have now will not be good for tomorrow. And everybody, regardless of whether you are a panelist or an audience member, will have to go through security.

Second, I thought many of you were crazy when you said it's too cold in here, but I can't feel my feet.

(Laughter).

MR. FRANCOIS: And until I become a Commissioner, they're not going to change the temperature, so dress warmly tomorrow, because they've told us they can't move the temperature up or down.

Finally, tomorrow morning we convene with

remarks from Commission Thompson at 8:15, and our panel will be the Economics of Spam at 8:30. Thank you very much, and we look forward to seeing you tomorrow.

(Whereupon, the hearing was adjourned).

C E R T I F I C A T I O N O F R E P O R T E R

DOCKET/FILE NUMBER: P024407

CASE TITLE: SPAM PROJECT

HEARING DATE: April 30, 2003

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the notes taken by me at the hearing on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED: MAY 19, 2003

SONIA GONZALEZ

C E R T I F I C A T I O N O F P R O O F R E A D E R

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

SARA J. VANCE