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 **MAY 2, 2003**

PAGES **1 THROUGH 343**

FTC SPAM FORUM -- DAY THREE

SECOND VERSION

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

---

1 FEDERAL TRADE COMMISSION

2 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: Well, this is the day we've all been waiting for when we figure it all out and then go home for the weekend. Before I introduce Commissioner Swindle, I want, once again, to recognize and thank the people who work at the Federal Trade Commission who have done such a magnificent job in every respect putting this program together.

The ring leaders are Brian Huseman and Sheryl Novick and Renard Francois; Jennifer Bernan from our Western Region has worked on this; we have a former staff member who was key, Lisa Tobin, with us; the lawyers whom I have the great good fortune of working with every day, Dan Salsburg, Eric Wenger, Steve Cohen -- who am I forgetting? Mark Groman, who is up later today and has been up. Just wonderful colleagues, and they have spent -- Steve Wernikoff, from our Midwest Office, Lisa Hone -- they have spent months reading up about you, and trying to assemble the richest and most varied panels to really develop a deep and broad record. And I just want to thank and recognize them.

(Applause.)

MS. HARRINGTON: And many other staffers at the FTC. We have our security people and our technology people and our press people and our business education people -- everybody has worked as a team.

So, you know, it's a great place to work and a great honor to work with all of these good people. And I wanted to just take a minute to recognize them.

Now, some of the other good people who we get to work with are Commissioners at the FTC, and you've heard from our Chairman and from Commissioner Thompson on the first two days. This morning we'll be hearing from Commission Orson Swindle, who has played a key role inside the agency in putting Spam front and center on our agenda.

Commissioner Swindle is one of the most amazing people I've ever met. Yesterday, he demonstrated, once again, the diversity of his expertise by playing Sergeant at Arms and subduing a little brawl that almost erupted here. So, we appreciate that. He is a retired Marine and he is a real -- he is such a clear voice for doing the right thing, and I think you'll find that in his remarks this morning.

So, Commissioner Swindle, thank you for being here and we look forward to hearing from you.

(Applause.)

COMMISSIONER SWINDLE: Thank you. It's nice to see everyone and thank you all for coming. The event yesterday, I came in late for the second session of the morning, and I missed some of the early verbal

confrontation and I was sitting right here and when lunch broke and being hungry, I was the first to leap up and start running for the door and I was caught in between two gentlemen --

(Group laughter.)

COMMISSIONER SWINDLE: -- Of somewhat smaller statue than myself, one slightly larger than the other. And what I didn't know was in the earlier conversations apparently these guys -- and I won't mention names and you can all pick them out if they're in the audience -- but they were nice when they calmed down, but they were rushing to confront each other and I just happened to walk in the middle of them, between them, you know. And they both bumped up against me and they started jabbing at each other, and one saying, he assaulted me, and I said, take a deep breath. I said, if you want to see assault, I can give you some real good lessons in it --

(Group laughter.)

COMMISSIONER SWINDLE: -- but this is not assault. So, anyway, the third day, I'm amazed this many are still alive, you know, given the tenor of some of the conversations yesterday. It's been fascinating. I've been trying to spend a little time over here and then we have this magnificent thing that -- can I mention a brand name? CISCO hooks us up and we can watch the proceedings

here live and distract me from everything else I've done, but it's been entertaining and, obviously, informative and I'd like to spend just a few minutes here.

We've talked a lot about complexities the last couple of days. In fact, my head's been swimming because there's so much complexity in all this. And I confess, very quickly, to not really understanding much of what's been said, but that's your job. My job is to try and inspire, and perhaps I can do that with such common-sense approaches.

Last summer I was engaged in reading a book entitled Tuxedo Park. How many of you have read it, by chance? We're got a lot of techies in here and surely you've read this book. One person? No people? My goodness. I would recommend you read it. It's fascinating reading. It's an account of some behind-the-scenes activities that took place in the early days -- actually, the European early days -- of World War II. It started about September of 1940 and it involved -- this is true -- it involves two very wealthy financiers in the United States who were scientifically oriented and they were concerned that America was not ready for World War II.

In technology we were way behind. If you recall, those of you who are old enough -- I think I may

be the only one in the room old enough -- but you've certainly read the British were in dire straits because they were being overwhelmed at sea; the submarine packs of the Germans were sinking shipping and shipping was their lifeline; and we were on the verge of having Europe lose the war in 1940.

And, so, we've got to do something. And the British had developed a magnificent device called a magneton (phonetic). If I remember correctly, this is way over my head, too. By the way, is Pete Wellborne in here.

MR. WELLBORNE: Yes.

COMMISSIONER SWINDLE: Where are you, Pete? Are you a Georgia Tech graduate?

MR. WELLBORNE: Yeah, I'm a Georgia Tech graduate.

COMMISSIONER SWINDLE: I was told to look you up. Now, I'm going to make a confession here, I am, too. I am not an engineer, so I have no idea what a magneton is. But, anyway, in reading this book, it was the guts of what would be radar and the British were well ahead of us and it was not an original idea, but they were well ahead of us and these financiers gathered together some incredible renowned scientists around the world.

The Europeans had come over fleeing Germany;

Einstein and others; Lawrence of Lawrence-Livermore Labs; just some brilliant people. And they got them in a room at Tuxedo Park, which was the estate of Albert Loomis, and they said, we've got to solve some problems and we've got to solve them fast.

And they got to work and their collective efforts led to the rapid development, sometimes in weeks -- and certainly within months -- of radar, air-to-air, air-to-surface, and early warning types of radar. The air-to-surface radar was extremely critical because it enabled planes to find submarines with their antennas stuck up and they were able to start sinking submarines, which kept the fleet from being sunk that was supplying Europe.

They were very much involved in fire-control systems for weapons, in building Oak Ridge, and, ultimately, the atomic bomb. They solved incredibly difficult problems in remarkably short periods of time.

Well, I finished reading this book and I was so impressed by the commitment of these brilliant and somewhat driven scientists and engineers working together, focusing on great problems and finding solutions to meet severe challenges and confront danger, I said, you know, we ought to try this again.

And, in a way, this was the beginning, back

then, of the technology revolution. I get a lot of Spam; those of you who communicate with me know I get somewhat enraged by Spam. I use e-mail a lot. I believe in communication because I think that's where we all learn, and because of liking e-mail, using it a lot and hating Spam, I'm frustrated all the time.

So, when I finished reading this book, I said to Tim Muris, I said, you know, Chairman Muris, you and I ought to call together a group of people who are involved in all this, put them in a room and tell them they can't come out until they solve this darn problem.

(Group laughter.)

COMMISSIONER SWINDLE: So, I told Tim that we ought to use the Tuxedo Park strategy and get these people to working. Many of the people we called in in early September last year -- I believe it was September -- are in this room or have been here and have participated in these proceedings -- ISPs, servers, computer companies, technology people, communication people -- everybody who's involved in all this, and we sat down and we had a discussion.

We challenged them to collectively find the solution to meet what I -- and I'm sure all of us would probably agree on -- of what I perceive to be a grave danger and a severe challenge -- somewhat not unlike a

long time ago -- and that challenge is Spam.

I know that many of you have been with me at conferences over the past several years where we've been in these wonderfully intellectually stimulating discussions on the deployment of broadband -- the killer ap. We were in search of the killer ap, and the killer ap was going to make broadband take hold and broadband would be everywhere and the world would be a greater place and everybody would be happy.

Well, so far we haven't found the killer ap for broadband in the sense that it was discussed. It's still rather expensive to use. But, I would contend, from a purely consumer perspective, that the only killer ap I've seen around is e-mail.

We've got 250 million people in this country probably using e-mail in one way or the other, directly or indirectly. Businesses rely on it, we certainly rely on it at the Federal Trade Commission, that is the killer ap. And guess what, folks, I mentioned the challenge, complicated problems, dire danger -- Spam is going to kill the killer ap if we don't do something about it.

So, Tim and I called everybody in and said solve the problem. We don't want your advice; if we ask for your advice we have to have a Federal Register notice and we've got to get everybody involved. We just want

you to solve the problem. Don't come back until you solve the problem.

Well, actually, they came back. We had two or three meetings, as I recall, between last September and the end of the year, and things are starting to happen. This three-day workshop, in which the staff, as Eileen said, has done just a remarkable job on, is a product of those early discussions. The staff's efforts have been rewarded by your attendance and your participation, sometimes wildly impassioned participation, but nevertheless you've been participating and that's what it was intended to do.

All of you, our staff and you who have been here, are to be commended, and I offer my personal appreciation. And, as I like to say, we're going to solve this problem bit by bit and it's going to be done through a continuance of dialogue -- no single law, no single new technology, no new initiative, no new meetings are going to solve this problem alone -- it's going to be solved by all of us coming together and crossing paths and bumping heads and having little confrontations like we had yesterday. These are the ingredients that are going to bring us to a solution.

But, the key to getting the solution is that every single day and every hour of every day we have to

make some progress. That's a fact.

I would like to think that the recently announced combined efforts of Microsoft, AOL and Yahoo to go after Spam is an outgrowth of those meetings. Now, I read one account that said they didn't know who brought this idea up of them getting together, and I'd like to think we had something to do with it. But, regardless of whose idea it was, the fact is they're getting together and I personally am expecting results -- not PR -- and I look forward to meeting with them on frequent occasions in the future to hear about how they're doing it. I commend them for getting it going. They're engaged in a dialogue.

Today's discussion will focus on Potential Solutions to Spam; specifically, legislation; maybe litigation -- do we really want any more of that? And technology -- and God knows that's got to be an understatement, for sure.

As complex as all this is, I believe I know a few things for certain as we search for solutions.

One, not one of these avenues -- legal, technology, political, you name it -- alone is going to solve this problem.

Two, we can never stop refining practices and searching for better solutions.

Three, we will never find a perfect solution, it does not exist.

Four, new laws that are unenforceable for a myriad of reasons, or that are overtaken by the advances of technology, have the potential to do more harm than they do good.

Five, and I would like to emphasize this and I will repeat it again. We need consumers and average users involved in this process. Awareness is essential. Without it, we get nowhere.

Six, we must get this right and get on with it quickly or we run the grave risk to the potential of the internet, e-mail, electronic commerce and, I might add with great emphasis, national security.

Seven, we must all work together to solve the Spam problem.

And, finally -- perhaps most important of all these -- this is a journey; it is not a destination. Political solutions, my own personal opinion, are oftentimes destinations. There is a clamor of great cries, do something, do something, do something, do something, at every even year, there are those compelled to do something. And doing something is often legislation, at whatever level. Once the legislation is passed amidst all the emotion, we declare victory and go

home, the dialogue stops, and we're getting behind the minute it stops.

So, we have a lot of work to do. This is a journey and not a destination.

I see two spheres of problems: One is very complex in terms of technology, the law, business models, relationships, intellect, politics and, of course, cost.

We've been addressing much of these complexities and these problems over the past two days. These problems and challenges will demand of you all considerable time, resources and cooperation to solve.

The other problem sphere is the one I want to talk about today and hope generate some discussion from our panelists. It involves the sphere of internet users and consumers. There are a hundred million or so here in the United States alone -- I believe someone mentioned yesterday, I think, that there are 600 million around the world, and that's irrelevant because it's growing every day.

This problem is less complex but it's more emotion. Emotion will kill you before facts will. These end users, these consumers by the millions, are absolutely getting fed up with Spam. If we turn them off, the consequences economically, socially and development-wise are going to be extremely serious. If

we fail to solve either problem's sphere, it bodes ill for the potential of this marvelous tool for growth and development.

It seems to me we are closer to failure we consumers, than we are with the more complex problems, at least from an economic and emotional standpoint. The damage will occur far more quickly, yet I have heard today, in this conference, very little, up to now, about helping consumers and avid users cope with Spam. It seems to me we could help them quickly and quell some of the frustration and quell it quite significantly.

I hope today's discussions will focus a bit on empowering consumers so that they might be in control, **THEY** might be in control of their inbox. They need the option, easily executed, at no additional expense, preferably, to block Spam. I prefer the word "nuisance" to Spam. I don't care if it's commercial, if it's religious, if it's entertainment, if it's jokes, if it's pornography -- it's all a nuisance to me, and I'm sure most consumers would probably agree with that. We need to stop that from entering their lives and frustrating them and turning them off to this fabulous medium.

I sometimes get the distinct impression that commercial interests of internet providers and marketers are reluctant to empower consumers. I just had this

sneaking suspicion.

(Group laughter.)

COMMISSIONER SWINDLE: Certainly, some of the remarks we've heard here have hinted of this. Firstly, I think the right to be left alone trumps what some marketing firms might think is its right to intrude regardless of my desires.

(Group applause.)

COMMISSIONER SWINDLE: May I suggest for beginners that ISPs try the Tuxedo Park strategy -- very, very quickly. Give the consumers the capacity to easily and inexpensively designate with a personal filter those from whom e-mails are acceptable. For example, the consumer's personal address book or any e-mail address they might choose to put in that personal filter that sits right here, before anything comes in. And if the incoming doesn't match what's here, it doesn't come in.

Now, some tell me, oh, you might miss getting an e-mail from a friend you haven't seen. My problem -- I'll take care of that. If that friend really wants to talk to me, guess what? They'll find me somewhere. But give the consumer something that simple. I am amazed, in particular with major ISPs who have done remarkable work -- and I'm not trying to pick on ISPs here, because everybody's at fault, this problem is an obvious problem,

it's been obvious for years, and we've been so obsessed with getting so far down the road and new bells and whistles that we've not taken care of security and privacy as we've gone along this path. And it's time to do that. It's past time to do it.

So, I'd like to see the ISPs and the servers who are providing consumers this service -- and I say providing, I think, you know, there's a fee associated with it. I pay for mine, some use it free. I don't think things should necessarily be free. I think if it costs something to provide this that that's legitimate. That's the American way. But let's put that shield out there so that, number one, we can quickly get to this sphere of consumers and users and the emotional fallout from their frustration -- let's get that taken care of as soon as we can.

We can do that fairly quickly, that will solve that problem, and then the genius of all of you, working together, working in conflict, beating each other about the head and shoulders and doing all these things that you do so well, using and deploying this immense talent that you have that has given us all this and you can solve the complexity sphere. But that's going to take a long time. But emotion can be handled fairly quickly if you do it right.

So, I would challenge you all to think in terms of empowering consumers. Once you do that and give the consumer, at his option -- he doesn't have to turn the thing on or he can turn it off -- but give them the option to put that screen out there to keep out all e-mail that he or she does not want to see. And the ISPs can have all that other stuff -- just don't send it to me; I don't want to see it; give me the option to easily take care of it.

And one of the first steps would be to make it possible to copy my address book -- this is a novel idea. I'm amazed that I came up with this.

(Group laughter.)

COMMISSIONER SWINDLE: To copy my address book, easily, and move it, with one click, to the filter. You know, I was with one of the biggest ISPs in the whole universe, and I can't do that; but yet, I can talk to Mars -- something's wrong here.

(Group laughter.)

COMMISSIONER SWINDLE: This gives you sort of the hint that maybe they don't want you to have that empowerment. And, folks, at the FTC, consumers come first and if you don't want an FTC in your future, don't mess with consumers.

We have a busy day ahead of us and as my

favorite Robert Frost said, "We have miles to go before we sleep." As I said, this is a journey and not a destination and, believe me, we all have to make this trip.

Thank you very much.

(Applause.)

MS. HARRINGTON: Thank you very much, Commissioner Swindle. As you see, we selected him for Day 3 because he doesn't have any opinions about anything.

(Group laughter.)

MS. HARRINGTON: Before we begin, let me ask you to please, please, please turn off your cell phones and remind you that if your cell phone rings, we will harvest the address and send you wireless Spam.

(Group laughter.)

MS. HARRINGTON: Is this a great technology and medium, or what? It's been brought to my attention that we have a news group called The Secret Diaries of the FTC Conference --

(Group laughter.)

MS. HARRINGTON: -- and if you go there, you'll read things about yourselves. But, here's one that came in the other day to me -- or about me. It's very interesting. "Any man that brave can drink out of my

canteen any time. You rock, rough and stuff with your Afro puffs and get down with your bad self, girl. When I'm king, you're going to be the Castellan that actually runs everything." Okay!

(Group laughter.)

MS. HARRINGTON: Keep it coming; keep it coming. Now, this morning we're going to discuss the key issues that everyone is wrestling with on the subject of legislation. Should there be legislation -- state legislation, federal legislation? What should it contain, what should the nature of laws be, should there be broad federal preemption, should there be an advertising, labeling requirement, should there be a private right of action, should there be criminal sanctions? These are the core issues, and we have, I think, a very good panel to help us explore those.

Jerry Cerasale is the Senior Vice President of the Direct Marketing Association, an organization that is much loved by all in the room, as we know from the other day.

We have Ray Everett-Church, who is counsel with the Coalition Against Unsolicited Commercial E-mail.

David Kramer, to my immediate right, is with Wilson Sonsini Goodrich and Rosati.

Chuck Curran, down on the end, is the Assistant

General Counsel at America Online.

John Patrick is the -- John, are you down there? John is the Chairman of the Global Internet Project.

Steve Richter is General Counsel for the E-mail Marketing Association.

Paula Selis is Senior Counsel in the Washington State Attorney General's Office.

And David Sorkin, to my immediate left, Associate Professor of Law at The John Marshall School of Law.

I think I want to really dive right into this, because the issues are numerous, important and meaty. We would note that there are now, I think, 29 states -- is that right -- that have enacted some kind of Spam laws, the most recent to be signed into law in Virginia just the other day, which criminalizes a certain kind of Spamming activity. There are a number of other states with legislation introduced this year. Of course, we have legislation pending in Congress and, as we've heard this week, there's more legislation expected to be introduced at the Federal level.

The laws that we've seen, both enacted and proposed, fall into several categories. Some have a private right of action, as well as Government

enforcement; others call only for Government enforcement; some require labeling; others don't; and we heard yesterday, particularly, I think some good discussion about labeling and whether it does any good at all. And that's an issue that the panel will touch on, but we've heard from marketers that the view is that labels don't do any good.

There are statutes, existing and proposed, that prohibit certain false aspects about Spam; false header information, for example. There are laws that prohibit all Spam.

So, we see a variety of approaches that have been taken, that are proposed and, I think, we'll just get right to it with a first question; and that is -- and I'm going to call on the panelists, in no particular order, and I'd really like about 30 seconds from you, just to give us a sense of your going-in position here.

Is a Federal law necessary in the United States; will it do any good?

Paula, why don't we start with you, speaking from your perspective as a State law enforcer. Is there a need for a Federal law? Will it do any good?

MS. SELIS: Well, let me start with, is there a need for a Federal law? Right now, I think, as Eileen pointed out, there are 29 laws on the books, and

Washington was the second state to pass legislation in this area. As with a lot of consumer protection-type issues, the states are usually the place where these laws first get passed. And what happens is you get essentially what becomes a patchwork of laws across the country. This happened in telemarketing, it happened in 900 numbers, it happened in credit reporting, and on and on. And what happens eventually is that those who are regulated eventually come to Congress and say, please, please legislate, because we can't deal with the patchwork of laws. And I think that's part of the impetus for this Federal legislation that we're seeing now.

Is Federal legislation going to work? Is it important in this area? Is it necessary? I think only effective Federal legislation would work, and what I mean by that is that as long as we have strong Federal legislation, the states will not need to enforce their laws. But if we don't, then state law is necessary. That Federal legislation should be a ceiling and not a floor.

MS. HARRINGTON: Thanks, Paula. Steve Richter, where are you on this?

MR. RICHTER: In support of Federal law. It's impossible right now to advise a client on either side of

the equation as to what rights they have when you have the example we use is that someone opts-in for receiving e-mail; they live in the State of Washington; and then someone sends them from New York, through a Nevada server, an e-mail and they now have moved to New Jersey. What law can you tell either of the parties -- the sender or the recipient -- what law they should follow?

And, so, I'm in agreement with Paula that a Federal law has to be done in order to have any kind of compliance, but it has to have some teeth, and I also see where the state agencies can enforce the Federal law.

MS. HARRINGTON: Okay. David Kramer?

MR. KRAMER: I absolutely think we need Federal legislation here. I think Paula Selis is quite correct that the impetus behind the state legislation was really to send a message to Congress years ago that this is a problem that cries out for a legislative solution. It is a classic case of tragedy of the commons in large numbers, in economics, creating a situation where no one has a vested enough interest to go after the parties that are responsible, while the parties that are responsible have every economic interest to generate massive quantities of Spam.

So, I absolutely think we need Federal legislation, but I completely agree with Paula that a

Federal legislation that does not effectively solve the problem will simply make the problem worse.

MS. HARRINGTON: Okay. Before I call on Ray Everett-Church, let me pick up on that qualification that Federal legislation needs to be effective.

As you continue to answer the fundamental question, tell me one thing -- if you're saying that there is a need for Federal legislation -- what would make it effective.

MR. KRAMER: The biggest thing that would make Federal legislation effective is a private right of action. Without a private right of action, Federal legislation will make the problem worse. There is only one way to deal with a large numbers problem, it is to empower the large numbers of us that are affected by this problem to take action, ourselves, to redress it.

Is everyone going to take action? Of course not. But we have a paradigm here; we have a junk fax law that was passed in this country in 1991; we have a problem, at that point, where our fax machines were flooded with faxes, almost rendering the medium useless. We passed a statute and, thankfully, today you can come into the office and get faxes and your fax paper isn't all strewn about the floor with ads for radio stations and dinner menus and so forth.

That statute worked because of the threat of private enforcement. The statute empowers people to sue for $500 to $1,500 for each fax they receive.

MS. HARRINGTON: Thanks. Ray?

MR. EVERETT-CHURCH: The Coalition Against Unsolicited Commercial E-mail was founded in 1997 on the premise that Federal legislation was necessary. The Coalition believes that a multiplicity of approaches -- including technical and economic and social and legal components are all necessary to address the problem. And, at that point in '97, the legislative angle had not been fully discussed or explored.

We have been working as an organization for Federal legislation throughout the intervening years, and, if anything, the arguments we made in 1997, at the Federal Trade Commission event to discuss Spam, are all the more relevant and all the more pressing and it's time for Federal legislation. We advocate an approach similar to the junk fax law. And an opt-in approach for unsolicited commercial e-mail because the cost-shifting issues that David mentioned are so similar in e-mail space without the governor of things like phone lines and fax paper, it costs no more to send that next 10 million e-mails than it does the first 10 million, as an incremental expense.

So, Federal legislation can effectively address what is a breakdown in the marketplace.

MS. HARRINGTON: Thank you. I'm going to ask if people can shorten it up just a little bit for me. Jerry?

MR. CERASALE: Federal legislation is required to be part of the solution for the problem we face with Spam. We need it. It has to be in conjunction with industry-working filters, ISPs and so forth. We think that what is necessary, as well, besides just the legislation, is resources to the Federal government and to the states to enforce.

MS. HARRINGTON: So, resources is your answer to what would make it effective -- one answer?

MR. CERASALE: There's more than one, yes.

MS. HARRINGTON: David?

MR. SORKIN: Well, certainly Federal legislation is preferable to state legislation. My concern really isn't so much the enforcement aspect as the substantive rule. Most of the state Spam laws, most of the bills that have been proposed in Congress are counter-productive, and if we're going to have a bad law, I think we'd be much better off with none at all.

If we're going to have a strong, opt-in law, then I think the law can be an effective part of the

solution.

MS. HARRINGTON: So, opt-in is a key element?

MR. SORKIN: Yes.

MS. HARRINGTON: John?

MR. PATRICK: Well, I guess I'm in the minority here. I feel quite strongly we do not need any new legislation. If we get any new legislation, it has zero probability of working. And it's very easy to forget that the internet is global and, in fact, Americans are the minority of users of the internet, and in the fairly near future, the use of the English language will be a minority language on the internet.

So, we have to think about here a communications medium that is unlike anything we've ever had before. It works exactly the same in Burlingame as it does in Boston or Berlin or Beijing or Bangkok. It's exactly the same. And, so, to impose a law at the Federal government means absolutely nothing to most people in the world. So, the laws really have no chance of working.

There are, however, solutions to Spam. I agree it calls out for legislation -- this is a very emotional thing, as Commissioner Swindle pointed out so eloquently. We all want something to happen, but legislation has no possibility of working. And I have some ideas on things

that will work when it's time to talk about it.

MS. HARRINGTON: Okay, thanks, John. Chuck?

MR. CURRAN: We've seen staggering viral growth in the volume of Spam messages sent to our users, and the primary face of Spam is sent by techniques of falsification and identity concealment, and Federal legislation is an absolutely vital component to bringing some deterrent to that viral growth and to the practitioners of those kinds of outlaw techniques.

That's really -- it's not just civil penalties that complete the enforcement picture, criminal penalties are also necessary to truly deter those who are continuing this vile growth of concealment and falsification mail.

MS. HARRINGTON: Okay, thanks. Since, as Paul notes, the states have really, as always, been the laboratory on this issue, as they've enacted state laws and then worked with those. I'd like to spend a little bit of time talking about the state laws, our experience with them, and a fundamental question: Have they had any effect?

I would note that one of the features common among many of the state laws is that Spam bear a label, an ADV label. We, the other day, announced the results of a study that we did, pulling a random sample of Spam

that we have in our datasets at the FTC, and we found that only 2 percent of the Spam in our sample bore the label. And, I think, we have to assume that virtually all of those Spammers were sending Spam, in part, into the states with the labeling requirement, California being one of them. It's hard to imagine someone sending a huge volume of Spam and sending none to California. And that was an interesting thing for us to see, that only 2 percent of our sample bore the label.

I wonder why that is and whether we can have some assessment, in concrete terms, of the effectiveness of various state laws. Now, the laws vary. Some have private right of action in them; some don't. Some have labeling; some don't. Some prohibit falsity specifically; others don't. So, we're talking about different components in terms of effectiveness.

Why don't we first talk about the labeling issue, and whether, in your view, the finding from our study is off or whether it's consistent. You know, what's the deal with labeling?

Who would like to start?

MR. PATRICK: I'll take a crack at that.

MS. HARRINGTON: Okay.

MR. PATRICK: If I'm a Spammer in Tajikistan, why do I care about any state of Federal law; whether

it's labeling -- why do I care?

MS. HARRINGTON: Okay.

MR. PATRICK: It's that simple. It really is that simple.

MS. HARRINGTON: The Tajikistan Perspective.

(Group laughter.)

MS. HARRINGTON: We've heard that. Do we have any of the other stands here?

MS. SELIS: I have a thought on that --

MS. HARRINGTON: The Seattle Stand.

MS. SELIS: The Seattle Stand, yeah. Actually, Washington does not have an ADV requirement. Our law simply prohibits deceptive headers, deceptive subject lines. But, I think, this points out something that David Kramer said, was you need effective enforcement; you need widespread enforcement; you need an active deterrent to keep people from violating the law. And, as long as it's more profitable for people to Spam and the risks are fairly low that there will not be the enforcement effort, they're going to go ahead and do it. It's an economic decision.

And if, in fact, there's effective enforcement, there will be an effective deterrent and the rate of Spam, those kind of violations, including the failure to put ADV, will slow down. But we haven't seen that yet

because we've only seen limited enforcement. Of the 29 states that have statutes on their books, I know of only three who have actually taken state action.

MS. HARRINGTON: Why is that? Why isn't there more active enforcement?

MS. SELIS: Well, you know, it's a variety of things. It has to do with budgets, it also has to do with the difficulty of actually filing cases, finding Spammers, the technical barriers. But, I think, over time it's going to get easier and the enforcement authorities will get better at it. Especially if there's right of action that is in the private sector. Private people will take action, too, and there will be massive enforcement and massive deterrent.

MS. HARRINGTON: Why do we think that private citizens will be more successful tracking down Spammers than government enforcers have been?

MS. SELIS: Well, some of them have taken action in Washington, and they face some of the same difficulties. But, in fact, some of them have been successful. And, in fact, some of them have sued the merchants who are selling via the Spam. So, it's not an impossibility. There are barriers, it's true, but I think with a widespread law, with an automatic enforcement mechanism, people are more likely to take

action.

MS. HARRINGTON: Some of my colleagues in this room -- Jennifer, Marc, Lisa, others -- spent 18 months going around the country training state and local enforcers on internet investigation technique. We got a lot of interest, we trained, I don't know -- Marc -- 1,750 local and state enforcers on how to do this kind of investigation. And, so, for us there's a little bit of a disconnect between the effort to put in that kind of training effort and the lack of enforcement at the local level of these laws.

Is there more that we can do to encourage enforcement?

MS. SELIS: As an agency? I think if there's a Federal law, and it's a good Federal law, and every state and every Federal entity -- the FTC and the states are working together -- there will be more cooperation. Because now when you've got 29 different laws; 29 different standards; and you've got the FTC, who doesn't really have a law to work with -- you're only working with your FTC Act -- I think you have a divergence of legal opinions and even if you understand the methods with which you need to investigate these cases, you have a disconnect over what law to use and what court to go into.

So, if there's a uniform standard, I think that's going to go a long way toward uniform enforcement.

MS. HARRINGTON: Now, when you talk about uniform standard, this is for Paul and all of you, that suggests preemption to me.

MS. SELIS: Um-hmm. And, as I said earlier, I don't have a problem with preemption as long as there is a strong Federal law and as long as that law makes it easy or relatively easy to take enforcement action.

MS. HARRINGTON: Okay.

MS. SELIS: And we can talk about the substance of that later.

MS. HARRINGTON: Okay. Chuck, what's the view from AOL about the effectiveness of state laws and, in particular, you guys have been big champions of this new Virginia law that criminalizes the most egregious kind of Spamming.

MR. CURRAN: We get millions of complaints from our members every day and we use them as evidence in cases. We find that the majority of those involve these kinds of techniques of falsification and concealment. The Virginia statute, like any other states, is focused on the kind of computer crime aspect of that, and gives both enforcement and civil remedies.

So, we're a big believer -- instead of either

or -- of both and -- that Federal enforcement remedies that are targeted towards the people who send the most objectionable Spam, by the most objectionable means, and in the greatest volumes, that's where you get the biggest -- when you were talking about effectiveness -- that's where you achieve effectiveness.

MS. HARRINGTON: Okay. Now, David, you're a proponent of private right of action in state laws and you have actually used private right of action in some of your work, what's your assessment of the effectiveness of state laws?

MR. KRAMER: I would say they have been completely ineffective, but I would say that if what the goal was was to generate interest at the Federal level, they've served their purpose. They were never intended to solve the problem. And, in fact, when a state acts in the context of interstate commerce, it needs to be very careful about what it's trying to do. A state can't ban all Spam on the internet because of Constitutional concerns with the commerce clause. So, states have taken a very limited approach to the problem, all their statutes reflected.

With respect to the issue of a private right of action, however, you will see private enforcement where it makes economic sense. Where there is a reward to the

consumer for serving the public interest by going out and taking action, if only for $1,500 in his or her own name against a Spammer, you will see an individual going to court and bringing those claims.

Right now, we don't have a lot of private rights of action over state laws that give individual consumers or individual businesses the ability to bring a lawsuit that makes economic sense.

MS. HARRINGTON: All right, now, if you talk about private right of action, we take a look at Utah, for example, where there are class actions being filed by one particular law firm that's, you know, demanding $10 per client; $6,500 in fees, you know, does private right of action open the flood gate for that kind of aggressive class action?

MR. KRAMER: Yeah. I mean, Steven can speak to this as well, but certainly that was an example of state legislation gone awry. The statute was not written with careful protections in it to ensure that what it was actually doing was fighting Spam and it has, instead, become a class action lawyer's full employment act in Utah.

That wasn't ever the intention, but it wasn't properly written. I think with, even, the least bit of careful drafting, we can prevent that problem. We see it

at the Federal level in the Fair Debt Collection Practices Act; we have limits on what class action attorneys can do when there's a private right of action for statutory damages, and any Federal legislation needs to have that kind of limitation in it.

MS. HARRINGTON: Okay. Can anyone on the panel point me to an example of enforcement of a state law or enactment of a state law that has achieved a demonstrable result in reducing the amount of some kind of Spam -- any kind of Spam? Is there any anecdotal or, even better, any survey-based evidence that anyone knows of on the effectiveness of any state law? Anyone?

MR. SORKIN: I guess I can speak to that anecdotally. I think state laws have done quite a bit to legitimize Spam in that nearly all of the state laws, in effect, authorize Spam that doesn't contain fraudulent headers, that has an ADV label and so on. And, so, I think the state laws have had an effect, but in the opposite direction.

MR. CERASALE: I don't -- with only 2 percent putting ADV, I'm not sure I agree with that statement. But, Eileen, I think the situation -- your study shows that at least two-thirds -- and I think Chairman Muris said that they didn't look further into the other one-third -- are people who are already doing something

fraudulent and the --

MS. HARRINGTON: No, our study said that there was likely false information.

MR. CERASALE: Likely false information. The incentive for them to try to follow -- outside of just being in Tajikistan or whatever the "stan" it was that we were concerned about, that that tends to be a problem in trying to get people to follow those state laws in a prescriptive type of labeling.

The other thing on the states, of course, is the problem -- and it's another problem that we should talk about today and how people obtain those addresses -- but, unlike the telephone, where state "do not call" lists and so forth work, where you know what state you're going into or a mail address -- a physical United States mail address has a state indicator, a geographic indicator -- an e-mail address does not, and we can -- how people paint it is another problem we should talk about today -- but that's another issue with state enforcement.

MS. HARRINGTON: Okay, anything else on existing state laws before we move on to some other topics?

MR. RICHTER: We all agree that they don't work, right?

MS. HARRINGTON: Well, I think what I'm hearing is there are certainly issues with ability to enforce, in terms of resources, in terms of locating, in terms of jurisdiction and venue. There are big compliance problems, obviously, and there are not strong incentives, perhaps, to comply. That seems to be the view.

MR. RICHTER: Eileen?

MS. HARRINGTON: Yes.

MR. RICHTER: I have a comment, since I'm very familiar with the Utah situation, and Utah is the poster child -- their statute in my mind is the poster child of what not to do if you want to make -- or what to do if you want to make sure you have no effect on giving any private citizen any rights.

And what's interesting in talking to their state legislators -- and the Utah bill was revised by the legislature in this last session -- but as the vote came to the final call, the clock struck midnight and their session ended. The government now has been urged by the President of the Senate and the Speaker of the House of Utah to call a special session for the sole purpose of revising the Utah law because it's a joke. And they all know because it's resulted in over -- right now I think it's over 1,600 lawsuits that have been filed -- and not more than $10 has ever gone into hands of any plaintiff

and over half of the plaintiffs are members or employees of the law firm that filed the lawsuits. So, it's an embarrassment to everyone.

But where I'm going with this is that we can look at the Utah situation and try to learn from it. What has gone on there, the theory of giving that Dave said, it's so important to give the private right of action to the citizen having the private right to act, but it has to be well done or the only people who are going to benefit are going to be the lawyers.

MS. HARRINGTON: Ray?

MR. EVERETT-CHURCH: A real quick comment. To say that state laws have been ineffective doesn't mean that there couldn't be more effective state laws, and I know from personal experience that Dave Kramer has drafted some good proposals, and has worked hard on that, and others in other states as well.

There could be more effective states laws, but what you see is a response in those states to Federal inaction on the issue, and you see an outcry from consumers, from voters, to address the problem, even if it is locally. And that lesson extends also to the global situation, as well, which indicates that even if Federal laws aren't effective globally, that doesn't mean that it's not a valuable thing to address it

domestically.

MR. CURRAN: And there's the part about drafting the statute and then there's the execution part. Certainly, in Virginia -- Virginia has tough and strong legislation -- but a lot has to with the execution.

Well, how do you actually prove the case? Where is the evidence? We, as ISPs, think that we need to do a better job of putting together the kind of various pieces of the chain of transmission, the evidence that enforcement agencies need to prove up the cases.

And I think this is an area that we can make progress in, working together, on the industry side. We have the evidence; we have the complaints; we just need to put it in the hands of state enforcement in an appropriate manner, such that the right kinds of large-scale Spammers can be identified and, then, actioned, under appropriate legislation.

MS. HARRINGTON: I know one issue that we in the Department of Justice and other enforcement agencies have been struggling with for the last couple of years concerns a balance between privacy protection in the Electronic Privacy Act and the hoops that we have to jump through to get that evidence from you that you have and our need to get it quickly. And that may be that's not the subject of this panel -- we're talking about Spam

legislation -- but there are certainly other existing laws that hinder the ability of law enforcement to quickly gather evidence that really need to be looked at.

MR. CURRAN: Sure, right. And there are many ways to balance those interests in gathering evidence and, then, kind of little acorns that are available for subpoena under existing processes. There's really, you know, thinking it through, there's really no reason why we can't balance both privacy and enforcement interests in an appropriate manner.

MS. HARRINGTON: Well, let's turn to the subject of possible Federal legislation. But let me say, again, that what I think I'm hearing from the panel is there are concerns about the effectiveness of existing state laws. Ray's point that perhaps state laws could be made more effective noted.

If there are such problems with existing state laws or if enforcement and effectiveness are questionable, why does anyone think it might be better or different with a Federal law? You know, is this just a matter of taking an idea that has been executed in the states that hasn't had demonstrable results and nationalizing it?

MS. SELIS: Let me speak to that here for a second. I don't think it's that the laws themselves are

bad in the states, I think that there is a problem with a lack of enforcement and a lack of resources. And somebody, I can't remember who, pointed out that in order to have effective legislation at the Federal -- and that goes for the state level -- you need effective amounts of money to fund it.

So, I think if there were a law on the books at the Federal level, it would have to have enough money behind it so that it would be enforced and, as Dave pointed out, there absolutely has to be a private right of action and there has to be an ISP right of action. Because the people who have the incentive to bring these cases are not necessarily the government authorities, but they're the ISPs and the individuals who are annoyed and harmed.

And if, in fact, all those things were present, I think what you'd see is more enforcement, therefore, more deterrent and more effect on the problem as a whole.

MS. HARRINGTON: Now, Dave mentioned the Telephone Consumer Protection Act, which prohibits junk faxes and has a private right of action in it, it also has a private right of action for telemarketing calls from companies that consumers have told to refrain from calling them.

Just anecdotally, my fax machine at the Federal

Trade Commission gets unsolicited faxes all the time. I don't know if the FTC has a private right of action under TCPA, but I'm interested in your observation that the private right of action in the junk fax and junk call laws has worked, because that wouldn't be my perspective from where I sit.

MR. KRAMER: I think that we have to go back in time 10 years and think about what it was like when you had a fax machine in 1991 to recognize just what impact the junk fax legislation really had.

MS. HARRINGTON: But do you think that it's the junk fax legislation or the widespread availability of the internet and e-mail? I mean, you know, faxing costs money; e-mail really doesn't. Has technology overtaken faxing as a popular marketing tool?

MR. KRAMER: Well, I certainly think that a marketer with the ability to send his or her message out at no marginal cost would much prefer to use e-mail than a fax machine. However, we still see fax marketing from time to time; people still think it's effective. It is a way of forcing your message into the hands of the unwitting recipient and forcing them to expend their time and their resources to deal with the message.

That's why we have a private right of action under the junk fax statute, and it's the same kind of

problem with respect to junk e-mail. It forces you to receive a message that you didn't ask to receive, it expends your resources and the ISP's resources with eventually no marginal cost on the sender.

So, in answer to your direct question, I think that the private right of action under TCPA has made a huge difference. I think there is, for lack of a better term, a cottage industry of enforcement springing up using the internet to gather information, with attorneys and individuals helping one another to bring these kinds of actions against telemarketers and junk faxers, and I think without that methodology, without that means of obtaining redress under a Federal statute, there's simply no effective enforcement mechanism. You're like the dog chasing the car -- what happens when you catch it? Nothing. And that's the problem we have today.

MS. HARRINGTON: Okay, as we continue on the private right of action and Federal law discussion, let me add to the question; and that is, if there were a private right of action, should it be in Federal court -- yikes -- or how would that work?

Jerry?

MR. CERASALE: I wanted to go back just a second to the TCPA and so forth and discuss private right of action. I think that private right of action for an

ISP to sue is also a private right of action. So, that I think when you think of that, we have to separate between citizens going to small claims court, et cetera, and ISPs for example.

And, under the TCPA, it is different because they use common carriers. So that there is a requirement to deliver, whereas in the internet context there can be -- and I think everything that DMA's worked on with any Federal legislation continues that right to filter for internet service providers, and so forth, and I think that that's a strong area where we can look to enforcement. They have the evidence, they know the big attacks on them and so forth, and we have to work in that context. So, I think it is different from the fax area in that context.

MR. KRAMER: I actually think it's worse in e-mail than it is in the fax context, because in a fax context the sender has a marginal cost and there's a natural limitation on the sender's ability to transmit his or her messages.

In the e-mail context, there isn't a marginal cost and the problem is exponentially worse. Beyond that, I think, the disruption that's caused by e-mail to businesses is one that's just not experienced in the fax context.

The massive loss of productivity in this country -- when an e-mail message hits the e-mail server at my law firm and it goes out to 2,000 people, the incremental loss of productivity from that single e-mail message is something that cries out for a legislative solution.

MS. HARRINGTON: Okay. Steve Richter, where are you on private right of action?

MR. RICHTER: I'm for private right of action in a court of competent jurisdiction, and what I want to do is allow the citizens to get into court without having to find an attorney and without having the attorneys profit. So, in most claim courts right now, their limitation, I think, is about $5,000 -- maybe some states a little bit less -- but I think everybody is leaning toward the $5,000. I don't think we're talking about a $5,000 fine, so where we're talking in the neighborhood of $250 or $500 per e-mail, you know, as a violation, let the consumer be able to go into a small claims court, file a $30 fee, and have their day.

You're going to get a lot more -- I really think what the Commissioner said this morning has to be taken at heart about let's protect the consumer in all of this -- and that's one way of the consumer letting the world know they're sick and tired of it. If they are a

silent minority or a silent majority, we won't know this, and we don't know this in Utah where 1,600 lawsuits are filed. The legislators there will tell you that they can't say that there's one less unsolicited personal e-mail coming into Utah because of the lawsuits, because the plaintiffs are getting $10 and the attorneys are getting $6,500. Who's winning?

MS. HARRINGTON: All right. It sounds like some on the panel, at least, would advocate for a private right of action for individuals in small claims courts; perhaps a private right of action for ISPs in Federal court. Is that the distinction that I'm hearing?

John?

MR. PATRICK: I think we're --

MS. HARRINGTON: John would not advocate for a private right of action.

MR. PATRICK: No, we're really kidding ourselves here, if we think that you can go to small claims court and sue this Spammer in Tajikistan. You cannot solve this with legislation. I don't mean to sound negative; I'm actually very hopeful right now -- more so than I've been in a long time -- about Spam. Spam can be solved; a private right of action is a technological action. It includes things such as Commissioner Swindle pointed out.

Personally, I don't want to eliminate any Spam unless someone's in my address book because I'm an author and a public speaker and I get e-mails from people I never met before and I like those e-mails. That's a good source of input for me.

But there are a lot of ways to solve this that are effective -- extremely effective. PC Magazine just ran a review of four different technologies that eliminate 99.9 percent of Spam.

MS. HARRINGTON: Well, John, that's a view that we're going to explore in great depth later today, but right now we're going to talk about legislation.

MR. PATRICK: Okay. I just want to say -- okay, since this is a legislative panel, so I won't make the technology plea. However, from the legislative point of view, you have to be able to define what it is you're legislating. And to talk about fax laws is really irrelevant. That's like talking about applying laws related to horses to laws about airplanes or cars.

E-mail was designed to be really, really simple and a lot of thought went into the protocol of e-mail to make it possible for anybody anywhere in the world to be able to send a message to anybody else anywhere in the world at very low cost and very high reliability. And, of course, that's what has made it desirable to the

Spammers. But it also makes it impossible to be able to pass a law that says you can't do that. It's like passing a law to say you must behave -- people must behave. You can't do it.

MS. HARRINGTON: Okay, Ray?

MR. EVERETT-CHURCH: If I could just respond to the Ambassador from Tajikistan.

(Group laughter.)

MR. EVERETT-CHURCH: The vast majority of Spam that gets forwarded to the Coalition Against Unsolicited Commercial E-mail is -- and please don't forward your Spam to us -- we get enough already -- but those complaints we receive are largely coming from servers, bounced off servers all over the internet -- all over the world. But still, the largest volume of that is advertising products and services that are being distributed domestically.

These are folks who may hire a Spammer who has a server farm in China, but who is still going to fulfill that order for herbal viagra out of their basement in Pasaic, and it's a bit of a red herring to focus on foreign relays if you still have a situation, which we have today, of the products and services being advertised largely domestic-based.

MR. RICHTER: Eileen?

MS. HARRINGTON: Hold on a second. I'm back with the image of the server farm in China. That's quite an image.

MR. RICHTER: I just want to say one of the things that also actually really speaks well that the lawsuits -- that there's validity in bringing them here in Utah, over 70 percent of the lawsuits filed have been answered. So, you know, I understand the issue of having servers in China and trying to avoid the lawsuits, but as we heard, the product is here and you can find someone to serve who is responsible for sending that e-mail. So, I really think we're chasing a rabbit.

MS. HARRINGTON: Okay. I want to shift to a different issue and that is the issue of preemption. If there were Federal law, how important is the preemption issue, how could it work without preemption?

Paula, would you like to start on that?

MS. SELIS: I'll jump in on this one, yeah. As Chris Gregoire, the Attorney General of Washington, said on the first day, there are 44 Attorneys General who have written a letter to the Federal legislators who are looking at legislation at this point voicing their opposition to a bill that would preempt the states.

That being said, I know that the Attorney General, at least of Washington, has said that if there

were effective Federal legislation, then the states would not have a problem or at least Washington wouldn't have a problem with preemption.

Now, what is effective Federal legislation? That's what it really comes down to. In looking at the Burns-Wyden bill, at least at this point, that is not effective Federal legislation, as the states see it.

MS. HARRINGTON: And why not?

MS. SELIS: Well, funny you should ask. Let me give just a little historical perspective on consumer protection law, and that, I think, will give you some frame of reference.

Before the days of consumer protection law, in order to show that one business has ripped off a consumer, you'd have to show fraud and for all of you lawyers and non-lawyers in the audience, let me say that fraud has a number of elements that you have to prove, including materiality and intent and knowledge and so on and so on and so on. And it became acknowledged that that was a pretty high burden and something else needed to happen.

So, hence, the creation of consumer protection law, which does not have such a high burden and, for the most part, only requires what we call a tendency or capacity to deceive, so you don't have to show intent,

you don't have to show knowledge, you don't have to show materiality and so for. So, it's a lot easier standard.

When we look at the Burns-Wyden bill and what does it do? It re-institutes all of the elements -- or at least most of the elements -- of fraud. So, in order to show a violation, you have to show that it was a material violation, that the violator had intent, that the violator knew that he was violating the law.

This, we see, as a step backward; especially since Spam is the number one consumer complaint these days, why give Spammers essentially what amounts to a lower burden than a higher one. I mean, it just doesn't make sense. So, I think that's an important reason that we oppose the bill.

The other reasons for opposing it have to do with loopholes and exceptions. And there's one in particular, I think, that we have an issue with and that is that there is essentially an excuse if the violator can show that he or she had what is called in the statute "reasonable business practices" then he or she can escape liability.

Well, what's a "reasonable business practice"? That means going into court, that means the Spammer is always going to pose that as a defense. Another defense is the Spammer's "good faith."

So, essentially, what this bill does is set us up for extensive litigation, court battles, they're going to last a long time, that aren't going to provide quick and effective deterrents.

And, finally, I guess we're going to wind up getting into controversy over penalties. The bill proposes a $10 per Spam penalty. In Washington we now have a $500 penalty, and I ask you if we're talking about deterrents is $10 a pop enough? I don't think so. We want to make it not worth the Spammer's time and effort to send the Spam, but at $10 a pop, it's basically the cost of doing business.

So, those are just a few of the reasons why at this point we oppose the legislation.

MS. HARRINGTON: You oppose Burns-Wyden. And we're going to talk about that, we're going to also talk about at least a couple of other proposals that we've heard mentioned here. One Representative Lofgren's bounty-hunting proposal; another Senator Schumer's proposal to create a national do-not-Spam legislation. Burns-Wyden is the one that's been there for quite some time.

MS. SELIS: Right. And a lot of those bills that you mention kind of jump off of Burns-Wyden and have a lot of the same elements, but I do want to at least

make sure that we acknowledge that the effort itself is a good one. That we applaud the effort of trying to put together decent Federal legislation, and there are some elements of Burns-Wyden that we think are good and we are, in fact --

MS. HARRINGTON: What are those?

MS. SELIS: I think the ADV label is a good one; I think the idea of having a notice --

MS. HARRINGTON: Why?

MS. SELIS: Well, it allows the consumer to filter. And I know there's some controversy about that and the effectiveness of that, and we can talk about it, but as a starting point, I think it's a good idea.

The notice and the ability to opt-out, we think are good, provided that they're effective and that there aren't any loopholes there, and we do have some concerns about that.

So, we think those are good places to start.

MS. HARRINGTON: Okay. Jerry, does the Direct Marketing Association support Burns-Wyden in its entirety?

MR. CERASALE: We support principle and approach. There are a few definitional things right at the moment that we would like to have straightened out, but, basically, we like the approach; we think --

MS. HARRINGTON: What do you like about it?

MR. CERASALE: Well, as we've heard from many of our members, many ISPs, the big things are the people who are lying and so forth, and we want to try to get out to the big push on that.

MS. HARRINGTON: Is the standard too high?

MR. CERASALE: Is the standard too high? I don't think the standard is too high. I think that the area of -- the other things in Burns-Wyden you must produce a physical address, show exactly where you are; you must have a unsubscribed -- say, hey, don't send me anymore, and it must work. Those are things that are not intent to fraud; you either have that or you don't. So, that, you have some of those issues that are added in.

The mistake problem -- there has to be something to look at on the mistake. This is your telemarketing sales rule -- has the mistake area pattern and so forth, and, you know, you do it two or three times, you can come after them and you lose the mistake.

So, we support that approach, and I don't believe there's an ADV label in Burns-Wyden, so that, I mean, we don't support that.

MS. HARRINGTON: What are the definitional problems that you have?

MR. CERASALE: Well, we want to look at --

there's some of the consent definitions that are there, we want to tighten up that definition and we want --

MS. HARRINGTON: You want more people to be able to receive Spam or fewer people, you know, let's get concrete here.

MR. CERASALE: Right, sure. We want the consent to specifically talk about notice and opportunity to say no, which I think they do have, but we want to make sure that that isn't confused; that also you obliterate the opportunity where someone says, I want to receive it. So, you have to make sure that your definitions include, from our perspective, people told us to say no and also people said, yes, I want to receive things. So, that we want to make sure that that's correct in that area.

And we also want to make sure we define, specifically, a little bit more tightly, the rights of the internet service providers to go to Federal court to enforce the civil side of Burns-Wyden.

MS. HARRINGTON: Okay. Thank you. David?

MR. KRAMER: I have a real problem with this legislation. It's unfortunate that it's called the Canned-Spam Act for short, because what it really is is the act that says "you can Spam."

(Group laughter.)

MR. KRAMER: It is legitimizing a practice that is reprehensible in our society. It's a practice of theft and this statute -- the problem isn't that Spam is fraudulent, the problem is Spam. I don't care that a message that I get is --

MS. HARRINGTON: Theft is a strong term.

MR. KRAMER: It's a theft of resources, it's a theft of my time, it's a theft of the ISPs resources for processing data, for storing these messages, and, obviously, we're not talking about one message when we're talking about theft, but one message is the tip of the iceberg.

The problem here is that we're codifying, with this legislation, a suggestion that it's okay to Spam as long as you do it within these certain rules. It's okay consumers, you're going to get 1,000 messages a year and you're going to have to opt-out of 1,000 lists that you didn't ask to get on in the first place, and there's no private right of action in any event, so, too bad, if you have a problem and they didn't take you off the list, tell the FTC and they'll take care of it, or tell your State Attorney General and they'll take care of it.

Not nearly enough with this bill. And while I again, like Paula, applaud the Senators for taking some action here, I think it's badly misdirected.

(Applause.)

MS. HARRINGTON: Okay.

MR. PATRICK: I want to strongly agree.

MS. HARRINGTON: Nice of you to bring your whole family today, David.

(Group laughter.)

MS. HARRINGTON: John?

MR. PATRICK: I want to strongly agree. This is wonderful that there's an attorney on this panel that I really strongly agree with. Because the reasons that he gave for why that bill can't work are going to be the reasons that no bill can work. And, so, I'm in violent agreement that private action really is the answer here, but it's not private legal action -- it's private action to not technically permit those e-mails to come into my inbox if I don't want them.

MS. HARRINGTON: David Sorkin?

MR. PATRICK: There's a lot of ways to do that.

MR. SORKIN: If I were going to draft the worse possible bill, I would probably do a few things slightly different than the Burns-Wyden bill did. It would take me awhile to figure out which things I would do differently.

(Group laughter.)

MR. SORKIN: I would probably draft a

preemption clause very much like the one I read in the bill, which preempts only the one strong state's Spam law and leaves all of the counter-productive ones and the one that's somewhere in the middle, which I would say is Ohio's -- it leaves all of those in place.

It creates a labeling scheme which, I think, many -- probably most of us -- agree is the wrong idea and, yet, the labeling requirement in the bill isn't even the standard method, so it wouldn't even work. It simply says a clear and conspicuous identifier, not an ADV label. If we're going to have to live with the label, at least we'd like one we can use.

So, I have to agree with Dave. I think the bill would be a large step in the wrong direction. But I do want to add, I think, to some extent, we're putting the cart before the horse when we talk about enforcement before we talk about what the rule should be. I don't really care that much about enforcement, I'm not crazy about the idea of having a Spam law that doesn't work real well that doesn't get enforced, but I think the real principle we should be following at this point is, do no harm. If we come up with a Spam law that might do some good and won't invite a hundred times or a thousand times or a million times more Spammers into the business, then I think at least we're starting to accomplish something.

MR. EVERETT-CHURCH: Eileen?

MS. HARRINGTON: Yes, Ray.

MR. EVERETT-CHURCH: Those of who've been involved in the anti-Spam activities for a long time, recognize Burns-Wyden as sort of the logical descendent of a proposal that then Senator Merkowski from Alaska -- the current Senator's father, I believe -- proposed and, in fact, was almost immediately taken up as a cause celeb by the Spammers themselves, citing the legislative proposal in their Spam. It even occurs still today, if you search your database, the FTC's refrigerator, for S1618, as authorizing this piece of e-mail, in most cases it wouldn't have if it wouldn't have if it had become law, but the Spammers took it up as something that legitimizes their activities, and Burns-Wyden would do the same.

MS. HARRINGTON: Okay. I want to talk about another fundamental question, and that is whether enactment of a Federal statute regarding Spam would put on the books a set of requirements that would be immediately outstripped and outdated by development of the technology. There's some concern about the ability of law -- and particularly statutory law -- to keep up with innovation and development in the technology.

Can you think of some sort of statutory scheme

that would be less likely to be immediately obsolete?

MS. SELIS: I have a suggestion on that and, in fact, Washington has a good example. Just this last session, we realized that not only a conventional Spam problem but text messaging, which is its own form of Spam, is a problem, too, and our legislature just passed a law prohibiting commercial text messaging. I think it might be the first one in the country, but it points out what Eileen just mentioned that you've got technological changes, sort of variations on a theme, and how are you going to keep up with them. And I don't think you can do by coming back to your legislature year after year after year with a new problem.

Now, the FTC, I think, is set up to deal with that far better than the states in what you have rule-making authority at the FTC, and if you wrote a statute that provided for rule-making at the FTC, which could allow for those changes, those subtle changes -- granted not wholesale changes to the law by the FTC, but something within the FTC's ability to change -- I think you'd have a built-in mechanism for some kind of flexibility.

MS. HARRINGTON: Chuck, you wanted to say something, it looked like.

MR. CURRAN: Yeah, actually, I don't think it's

necessarily as great a challenge. There's a problem with drafting to technology if you get lost in the weeds of the technology. However, if you, you know, certainly from the kinds of what I call the outlaw Spam, the fundamental activity is the acts of falsifying your location and your identity.

Technologies may vary, but if you draft to the fundamental act that's occurring, basically people are engaging -- concealing who they are, what they're doing, how much they're sending -- in order to trick ISP and individual consumer filters.

So, I think you can anticipate new technologies by simply saying it's the act of concealment, you speak to those by-whatever technological means.

MS. HARRINGTON: Do you suggest that the volume issue is one that should be left alone -- legislatively/ statutorily?

MR. CURRAN: The volume issue is a very difficult issue because, certainly, every day, seven by 24, the Spammers are out there on a technology side testing whatever filter -- if you say the number is 10, they're at nine; if you say the number is 100 -- and the nature of SMTP -- mailing protocols -- allows mail transmissions to be broke up into so many little packets that mail, as sent by sophisticated Spammers today,

generally comes in in a kind of diffuse cloud. It's very difficult to identify one source.

So, you know, trying to hit a number is something of a drafting trap. It encourages Spammers to just come up with one more game to beat the number somehow. But once, again, if you draft creatively with keeping an eye on the fundamental objective, you can reach the act.

MR. PATRICK: I disagree.

MS. HARRINGTON: Who said that?

MR. PATRICK: John.

MS. HARRINGTON: John?

MR. PATRICK: You really can't. I mean, we are moving into a world whose identity is going to be extremely difficult to define. Is it our virtual identity? Is it our wireless identity? What kind of identity are we talking about? And you can't define that from a legislative point of view.

You can define, however, content. And this is what's working today is that, although the techniques that were just pointed out, are happening in terms of randomizing the to address and the from address and the subject line and so on, the basic content of the message is basically the same.

And, so, collaboratively, if 1,000 people got a

message that contain service, similar kind of message, then it's probably Spam. And those are the techniques that are actually working. And people that use them don't get any Spam. It's just eliminated.

(Mixed applause.)

MS. HARRINGTON: Ray?

MR. EVERETT-CHURCH: I agree with Chuck that the minute you start trying to define technical processes and standards in legislation you slide into a morass. But legislation can encourage the adoption of certain approaches by granting safe harbors to those who adopt those approaches, by encouraging the use and creating some penalties for things like new technologies that may come down the pike that enable a better statement of identity, statement of content.

We'll see some proposals later today and the Coalition has endorsed one proposal that you'll hear, the Trusted E-mail/Open Standard, which would enable senders to state identity in a secure way; to state content assertions in a verifiable manner and legislation that encourages adoption of those standards and punishes the misuse of identity and misstatement of assertions, could encourage solutions, including better technical solutions without getting lost in the technology morass.

MS. HARRINGTON: I see people are getting a

little restless, and we're not going to take a formal break right now, but let's involve some of you in the discussion for a moment. Let's go to the video.

Steve, are you there with your mic? Great. Steve and Sheryl, you didn't know we were going to do this right now, not a problem.

Okay, Steve, let's go to this gentleman in the white shirt right here for a question for the panel.

TOM: Two points: One, you can tell the country where a packet of IP comes from, technically. So, if all the Spammers are in Tajikistan or China, we can filter. That's number one.

Number two, I believe that there is a scam behind every Spam. This is a law enforcement issue and we've got to give the law enforcement people the tools that they need to go after these organized crime.

MS. HARRINGTON: Okay, thank you.

TOM: And just, finally, I'd like to suggest the U.S. Postal Inspectors. They're doing this thing for the mails today. The rules say that they go after things that go through the physical post. The same exact job needs to be done online. They've got the tools, they've got the competence, give them the mandate for cyberspace.

MS. HARRINGTON: Okay. This gentleman, Sheryl, right here.

DAVE CROCKER: My name is Dave Crocker, Brandenburg Consulting. I wrote a fair portion of the internet technical standards for doing e-mail. So, this is a fairly interesting topic to me.

There's a peculiar mix coming from the table up there. One thing I would encourage people is to pay a lot of attention to the cautions being raised about the degree of control that is available. There was an observation made that making state laws is more for the purpose of getting Federal interest, because of the scope issue -- the scope of control.

That is worse for Spam than it is for fax, because Spam can come from anywhere. There is an observation that generals tend to fight the last war -- we need to be careful that when we pass laws we're not fighting the last Spam.

Spammers are extremely adaptive. The things that work today -- I'm sorry -- the things that worked yesterday do not work today. The comment that content filters work today was true for me six months ago and useless today. The more adaptive techniques that are coming around in content filtering are much more powerful, but we are in an arms race if we take that approach. I think we need to take that approach because we need an array of tools.

My own view about Spam is that we need to view it the same way we view fighting roaches. You don't get rid of roaches, you bring them under control and you don't use one technique, you use an array, and you keep changing them over time because the roaches keep adapting.

So, let me suggest that there is a major value in legislation and the value is to create some very clear terminology that people will use consistently. And you may notice that is not yet true.

And the second is it creates some very clear guidelines for what's acceptable and what's not, because as we talk about Spam, we need to remember subscription mail, which in every technical detail looks exactly the same as Spam.

MS. HARRINGTON: Thank you. Is there anything in the mailbox? Brian, do we have some e-mail?

MR. HUSEMAN: Yes. Eileen, we have one comment, rather than a question. Why is the unsolicited bulk e-mail problem any different than the issues addressed by the existing fax advertising laws? With the existing fax advertising laws, we are not required to submit our fax machine number to an opt-out list.

MS. HARRINGTON: Any comment on that comment, from the panel?

MR. KRAMER: Yeah, it isn't, is the short answer to the question. The problem is almost exactly the same. I would suggest that it's far worse, in fact, in the context of e-mail, as I did previously, and I think the solution that we came up with as a society in 1991 here ought to be the solution that we come up with to this problem in 2003.

MR. CURRAN: And Professor Sorkin wrote a definitive Law Review article saying that the TCPA can't, unfortunately, be stretched to cover Spam, but makes some really interesting arguments about how to do it.

MS. HARRINGTON: Okay. We're going to come back to you with your questions and comments in a minute, but I want to move to a couple of suggestions that we've heard from your legislative components in the last couple of days.

First, we heard from Representative Lofgren about her bounty hunting suggestion on Spamming. Does everyone on the panel know what I'm talking about?

That's all around. Okay. What do we think?

MR. KRAMER: The San Jose Mercury News, which is a very tech-savvy paper in Congressman Lofgren's district, panned it twice. Basically, the Mercury News thinks that a TCPA-like legislative solution is the appropriate one.

The problem with Congressman Lofgren's legislation is that it's solving a problem that really isn't the problem. I have never had a problem finding the person I wanted to take action against. The problem was, an economical matter, it wasn't justifiable for me to sue that person. The person who is sending you Spam wants to sell you something, and with a little social engineering and a little investigation, you can almost always find out who that person is, if you want to take action against them and if there's enough economic justification for doing so. If you invest in resources, you are more often than not going to find the person.

MS. HARRINGTON: Let me just take issue with that, David. I think our people are as nimble and skilled as any in finding Spammers, but there's a certain category of Spammers who are not trying to get money, and they are very difficult to find. You know, law enforcement can follow the money, but if people are doing, you know, nasty and, you know, pranksterious things that impose significant cost but they aren't trying to collect money, then they are hard to find.

MR. KRAMER: Agreed. No, this is not a complete solution to the problem. I agree with everyone that has said that this is one of the tools that we need in the arsenal in the fight against Spam. I do not think

that any kind of legislation is going to eliminate the problem. I do think it will help bring it under control and that we ought to be thinking about ways we can do that.

The concern that has been expressed that you can't find these people, is simply a red herring in a lot of cases. In a lot of cases, you can find these people and you can't take action against them.

MS. HARRINGTON: Okay. Anyone else in the Lofgren proposal here? We're not going to hear from -- keep your hands down out there right now -- we'll come back to you, don't worry.

MR. RICHTER: I would just add that, you know, anybody can learn how to track down Spammers. I have a free website for people -- privacyfordummies.com -- has a tutorial that can teach anybody how to do what Congressman Lofgren is encouraging. The problem, again, isn't finding the Spammers, it's getting law enforcement to act or to have a private right of action for an individual to act.

The other component is --

MS. HARRINGTON: Well, where are you then? Representative Lofgren would say that, I would imagine, that her proposal would make it easier for law enforcers because people would be out there turning in these bad

Spammers.

MR. RICHTER: Well, I think --

MS. HARRINGTON: Do you like this idea?

MR. RICHTER: -- the FTC's -- I don't like the idea. The FTC's own UCE@ftc.gov mailbox is proof positive that there's no lack of complaints about Spam out there. You can find Spammers relatively easily, although there are evidentiary requirements to bringing an action that even state Attorneys General have difficulty meeting.

So, I don't see that an individual, unless you're somehow going to encourage people to hack into systems and find the kind of data that it takes subpoenas to otherwise obtain. Without that kind of action, you're not going to get any more useful information by creating a bounty.

So, I would agree with David, it's a solution for a problem that doesn't really exist.

MS. HARRINGTON: Is there anyone on the panel who wants to speak in favor of Representative Lofgren's approach?

(No response.)

MS. HARRINGTON: Representative Lofgren, we love you, but the panel doesn't love your proposal.

Let's turn to the Schumer approach, which

suggests the creation of a national Do Not Spam Registry that the FTC would run and --

UNIDENTIFIED SPEAKER: Lucky you.

MS. HARRINGTON: -- yeah. But Representative Schumer said that if this becomes law, we're going to get a lot of money to do this. And all I can say is, we would need it.

MR. SORKIN: Let me suggest a really easy way that the FTC could run that registry: Allow the listing of top-level domains, like .com.

(Group laughter.)

MS. HARRINGTON: And who would have the authority to register the domain?

MR. SORKIN: Preferable anybody but ICANN.

(Group laughter.)

MS. HARRINGTON: Okay, there's a thought.

MR. PATRICK: Eileen?

MS. HARRINGTON: Yes? John?

MR. PATRICK: Yeah, on this registry, it's a tempting idea. Many of these ideas are tempting and they're well-founded sort of philosophically, but they just -- they're not practical. I mean, look at the challenge --

MS. HARRINGTON: Why? Tell me really concisely, why this isn't practical?

MR. PATRICK: Well, because people change their e-mail addresses all the time; ISPs fold, new ones come up. We can't manage security very well in many instances, what makes us think we could do this? There are things much simpler than this that we can't do.

MS. HARRINGTON: Why is it significant that people change their e-mail addresses? Say, that I change my e-mail address every month and register my new e-mail address every time I change it. What's the problem?

MR. PATRICK: Well, again, it's just not an American problem, it's a global issue. People don't like Spam anywhere in the world, and trying to solve this at a local level, which is America, is just not practical. It doesn't address the entire issue.

MS. HARRINGTON: Well, we'll have a separate workshop on the Tajikistan --

(Group laughter.)

MS. HARRINGTON: -- and there's actually an international panel following, and I think that these are some of the issues that they will deal with, but Jerry?

MR. CERASALE: Well, unlike the telephone, where a do-not-call-list works, has worked in the states and so forth, and even the DMA list has been around since '85, where the fraudulent people were in telephone marketing or on the fringe, it's the legitimate marketers

that are on the fringe and the simple core are fraudsters, in essence.

And they're not going to follow. And, so, I think that you have a problem that it's not going to work because the basis of the users are not necessarily law abiding.

The other thing, from a marketer's standpoint, raises a real problem for us -- and we've seen this in part with even exemptions in phone lists -- if it doesn't work, that the fraudsters don't use it, and you put out -- we have this national registry and Jerry Cerasale enters the registry, I assume that's going to work, it's going to stop Spam, and I'm going to get inundated with it, still, plus the legitimate marketers will use the list, we're still going to be painted with the same brush that we don't even follow the law.

And, so, I think you have that kind of a problem. You don't want to set up that list when there is little likelihood that it's going to be successful.

MS. HARRINGTON: Well, would the purpose of this kind of law be, do the panelists think, primarily to reduce the volume of unwanted Spam or to provide an easier enforcement hook for law enforcement?

MS. SELIS: Well, actually, that's exactly what I was going to say. Looking at the state as a

laboratory, when we created a do-not-call-list, what it did for us is that enforcement authorities -- it enables us to go in and file what's called a summary judgment. We didn't have to prove anything, all we had to show was that Joe Blow's name was on this list, he got the call anyway; therefore, a judgment in favor of the state.

And I think that's the utility of having a do-not-Spam list, it enables the enforcement authority to go in and get a pretty quick judgment against the Spammer without having to prove more.

Jerry does point out something that I think is important, and that is that when you have a list, it creates an expectation on the part of the consumer that he or she is not going to receive Spam. When they do, they get angry. They think, gee, I thought this law was out there to protect me, and it's not.

So, there has to be some important consumer education that goes along with it.

MS. HARRINGTON: Okay.

MR. PATRICK: It's a database management problem, also, in that -- that's what I mean by it's not practical. I mean, when American Express sends out an e-mail every month to tell you that it's time to pay your bill, they send out very large numbers of these e-mails. UPS is one of the largest e-mail generators in the world;

and FedEx and Airborne. So --

MS. HARRINGTON: The point being perhaps if there were such a law, there would need to be an exception for e-mail from --

MR. PATRICK: Yes, I mean, this is a human cry right now, from associations, for example, the IEEE, or the Association of Computing Engineers or, I mean, there's thousands of associations, as you know. Right here in Washington there's thousands of them. They all have e-mail newsletters. All companies are moving toward legitimate e-mail for purposes of customer service; for purposes of order acknowledgment.

MS. HARRINGTON: Well, this gets us back to the definitional issue that we discussed on the very first panel; and that is, if Spam is defined in the law as including unsolicited and bulk, and we look further at the solicitation definition to exclude, you know, membership --

MS. HARRINGTON: Pardon me?

MR. PATRICK: You can't define it. I mean, American Express' monthly statement is bulk, unsolicited e-mail.

MS. HARRINGTON: No, not necessarily. If there's a contractual relationship --

MR. PATRICK: Well, it's --

MS. HARRINGTON: -- or an existing business relationship, I mean, there are ways --

MR. PATRICK: That's the point. I mean, so in this database we have to have a field to say, well, this particular case is an exception because there's a contractual relationship. Who's going to administer this database?

MR. SORKIN: This is exactly the case where the law can do better than the technology can in defining things like unsolicited.

MR. PATRICK: Not really. The only person that can define Spam is the recipient. Nobody can define it, but you know it when you see it.

MR. KRAMER: That's why you have laws.

MR. PATRICK: The law defines what Spam is, and if the definition in the statute is unclear, that's why you have courts. Why don't we define pornography?

MS. HARRINGTON: Excuse me, all right. We're going to continue on this discussion of the do-not-Spam with original thought here.

MR. KRAMER: I actually think that short of a ban on unsolicited commercial e-mail, that a do-not-Spam list in which I can put my name and know that having put it there I should not receive, and if I do receive any further unsolicited commercial e-mail, that it's a

violation of the law, if it gives me a private right of action, I am in support of that -- short of a complete ban on unsolicited commercial e-mail, because it doesn't put the burden on me to opt-off of all these lists and it does give me some measure of comfort, at least knowing that this will reduce if not eliminate unsolicited commercial e-mail. I don't think any of us can say that putting your name on a list is going to completely stop this problem, but it will help bring it under control.

So, short of a ban, I think this makes sense.

MS. HARRINGTON: Ray?

MR. EVERETT-CHURCH: I have severe concerns about the logistics of how a list would be operated. I'm all in favor of giving you lots more money, though, Eileen, so --

(Group laughter.)

MS. HARRINGTON: David?

MR. SORKIN: I think, in theory, or at least in looking at some of these proposals in the most charitable light, they may end up merging into an opt-in regime, if we have a do-not-e-mail list that contains every e-mail address of everyone who doesn't want Spam -- it's hard to imagine a database large enough to hold that -- but if we have such a list, or if we have an ADV law that requires an ADV label on every Spam and every internet provider

declines to transport any e-mail that has that label, and we allow them to do that, then what we effectively have is a legislative ban on Spam that doesn't admit that it's one.

Or if we have a law that says every internet provider has the authority to enforce it's anti-Spam policy as long as they post it on a webpage somewhere -- which we almost have in Ohio, but not quite. Again, we have something that becomes the equivalent of a ban on Spam -- an opt-in law.

Now, I think it probably has the same potential Constitutional problems as such a law, so I don't think it gets us around that question, and it's certainly less efficient, but if that's possible, then we may have another way of doing an opt-in without really admitting that's what we're doing.

MS. HARRINGTON: Okay. I'm going to turn to the big brain in the back row, Brian, do you have any questions that you'd like to hear the panel talk about?

MR. HUSEMAN: I do have one kind of technical question about the Burns-Wyden, but I think it is an important point. My understanding of the current draft is that the requirements that messages include an opt-out notice and, also, a physical address, those requirements only apply to unsolicited commercial messages. And I'm

wondering what is the panel's view on whether those requirements, including requiring messages to have an opt-out, should apply to all commercial messages rather than just unsolicited messages.

MS. HARRINGTON: Okay, Jerry, you get the first crack.

MR. CERASALE: Like I said, we support Burns-Wyden, but we believe that every commercial message should have an unsolicited and should clearly state who's sending it with a physical address where they can find you; physical address does not include a post office box.

MS. HARRINGTON: So, should apply to all, is the DMA view?

MR. CERASALE: Should apply to all.

MS. HARRINGTON: Chuck?

MR. CURRAN: I think as a matter of practice today, all commercial e-mail from the reputable senders contains opt-out messaging, just sort of mainstream companies are using that.

So, I think Burns-Wyden is about baseline standards and I actually disagree with some of my colleagues, I think they've done a good job in defining and attempting definitions of Spam.

But, you know, Burns-Wyden doesn't necessarily have to address -- as a matter of ISP practice, we can

set our own policies as well as it relates to certain kinds of desirable practices that we'd want to see.

So, I don't think it has to be necessarily decided entirely as a matter of legislation. Obviously, companies and technologies that can be developed that would kind of signal that perhaps higher practices are being followed by the sender, and those could be passed on through to the recipient.

So, you have to -- there's not just a legislation option, but there are also technology options.

MS. HARRINGTON: Ray?

MR. EVERETT-CHURCH: From the consumer point of view, having the ability to identify the sender is a very valuable thing, not only for weeding out the folks that you distrust, but for being able to recognize the folks that you do trust. That you see a communication from somebody that you recognize you have a relationship with, and that there is some recourse, some ability to contact them, as well as a standardized opt-out mechanism. That's something that technology can provide, but a baseline requirement of all commercial e-mail having some sort of standardized mechanism for removal would assist consumers very greatly.

MS. HARRINGTON: Okay. Steve Richter, should

those provisions of Burns-Wyden apply to all, not just unsolicited?

MR. RICHTER: Yes. In order to become a member of EMA, you have to subscribe to doing that. So, absolutely in favor of it.

MS. HARRINGTON: Okay, David?

MR. SORKIN: I suppose it makes sense. I don't think they help as much to deal with Spam, but I don't have any problem with them. I suppose I'd also say we ought to do it in a medium/neutral way and require all direct advertisers to identify themselves and provide people with a way to get off the list or stop receiving the junk, regardless of whether it's e-mail or telephone or door-to-door or direct mail.

MS. HARRINGTON: Well, now, there's the DMA's worst nightmare.

(Group laughter.)

MR. PATRICK: Eileen?

MS. HARRINGTON: Yes?

MR. PATRICK: May I comment on that same point? Yeah, I think it's a really good, sensible business practice to provide opt-out and to also provide an easy way to communicate back to the business. But, again, to define that through legislation is really not a good idea.

There are many entrepreneurs in the world today who operate out of their home, have legitimate businesses, who do not necessarily want to reveal their physical address for their own personal security reasons. They may be a consultant providing advice and very successful at it, and they have a right to be able to participate in that kind of business.

So, the market can regulate this and consumers can select businesses that they want to do business with, based on these kinds of features, but to legislate it and define how an address should be specified or how the opt-out should work, would limit the innovation that's possible. We're only 2 percent of the way into what the internet offers, so why try to define how it should work?

MS. HARRINGTON: Brian, is that satisfactory for you?

MR. HUSEMAN: Yes.

MS. HARRINGTON: Good. All right, I want to shift to a different question, and that is whether there should be criminal sanctions for some kinds of Spam. I think what we've been talking about so far are legislative proposals and, for the most part, except for Virginia state laws, that impose civil or administrative sanctions on those who violate or would violate these statutes.

Is there a kind of Spamming activity that should implicate criminal law? Chuck, you guys have been like major proponents, out in Virginia, of this new law.

MR. CURRAN: Yes, there are the people we believe are responsible for the greatest volume and the most objectionable Spam consistently use any number of techniques of falsification or stealing other's accounts, we think of it as a kind of computer crime. And I might add that Virginia is not the only state to have laws.

Many other states do recognize the sort of criminal element to the large-scale behavior that's going on. I think Connecticut, Arkansas, Illinois, North Carolina -- there's a school of thought in the states that this is a particular kind of problem that is recognizable as an act of using method of concealment to get stuff through and appropriate advertising resources. It's a form of theft -- burglary tools.

MS. HARRINGTON: What would the triggers, you know, be for imposing or possibly imposing criminal sanctions?

MR. CURRAN: I think they probably boil down to three concepts: One is just a flat-out falsification of header or transmission information to conceal identity and scope of mail.

MS. HARRINGTON: And doing that intentionally

would be the intent to falsify?

MR. CURRAN: Yes, that's right. Secondly, certainly if I hack into hundreds of people's accounts, take them over, take over my grandma's account on AOL in order to send mail, which is not dishonestly addressed, but obviously not from my grandma, that's a form of hacking that's a well-recognized defense.

And, finally, third you see the systemized taking over of free e-mail accounts by the hundreds for the purpose of disguising mail transmissions.

So, yeah, we believe that there's a clear pattern of activity that supports the large-scale Spamming and that it can be reached, obviously with appropriate gradations, obviously, not just one mail should be a felony, but with appropriate tiers and triggers reflecting the amount of money or the amount of mail sent. It's possible to appropriately define offenses in the same way we do for many other crimes.

MS. HARRINGTON: Thoughts on criminalization? Paula?

MS. SELIS: I agree with what he said, I agree with that. I also think there's a practical issue, though, that we can't really ignore and that is whether prosecutors are going to take these cases.

It's all well and good to have a law on the

books, and the question is what are the competing problems that those prosecutors are having to grapple with -- budgets, other cases that involve physical crimes as opposed to property crimes. And the perception, unfortunately, that the big guys, you know, the ISPs might be able to take care of themselves in the civil arena.

So -- and I'm not citing anybody in particular for having that position. So, I think that it might give you a sort of false sense of security in some sense to have a criminal law on the books, but the practical reality may well be that a prosecutor -- Federal or state prosecutor -- may not have resources or time to take those cases.

MS. HARRINGTON: Other thoughts on the issue of criminalization? Jerry?

MR. CERASALE: The DMA supports AOL and it's approach here, as we take a look at it. One of the things that -- and this is beyond our panel here, so I apologize for 30 seconds -- I think, as another facet of how we can go after Spammers is -- and we're starting to try and do this -- is to get together with ISPs and even law enforcement, to see what kinds of things can marketers, ISPs do, to gather information to give to prosecutors to assist them, in both civil and criminal

cases, to help them put together a case, in part. And there are a lot of legal issues and so forth, and we're just starting that.

But those are some of the things that we're looking at, as well, and I think go beyond the legislation but we'll try to answer the issue there of resources and effort to try to help in that sense.

MS. HARRINGTON: All right. I'm going to shift for a minute before we go back to our wonderful audience members for questions, and ask each of the panelists to take full advantage of the fact that we have C-SPAN with us together and perhaps, in addition to Congressional staffers who are here, we have members who are watching.

There's been a great deal of discussion, I think on-line and off-line, about Federal legislation and whether, ultimately, it will make matters worse, not better. And, certainly, all of us who work in the public policy arena sometimes view the process of developing legislation as being similar to that of making sausage.

I think that I'd like each of the panel members to look right into our camera and give us 60 seconds of your most fervent wish and intent with regard to Congressional action on legislation. What is the thing that would be a disaster; what is the thing that you most want or wish; what would say if you hold the pens of the

members as they write and draft?

And I'll ask for a volunteer to go first on this, instead of putting anyone on the spot.

MR. SORKIN: I'll go first.

MS. HARRINGTON: Sixty seconds.

MR. SORKIN: I'll take less than that, do no harm and opt-in. If you can't do anything other than opt-in, leave the technologists to do what they can.

MS. HARRINGTON: David, excellent. Who would like to go next?

MR. PATRICK: I'll go. Sixty seconds.

MS. HARRINGTON: John?

MR. PATRICK: Well, I would suggest put your pens away.

(Group laughter.)

MR. PATRICK: We do not need legislation, and this is a time to be very optimistic -- very optimistic, actually, about Spam. There are a lot of good things happening. Commissioner Swindle pointed out that three of the major internet service providers are getting together; they're competitors and they're getting together and talking about this.

MIT recently held a technology conference and some of the smartest computer scientists in the world are really intrigued by this problem, and they have a lot of

good ideas.

Venture capitalists see this as an opportunity to make money. Wherever there's a problem, there's a chance to make something out of it. And, so, they're investing in companies that are actually doing the roach approach, that the gentleman in the back talked about, and it's working.

It is a moving target, but they're moving very quickly on this, and there are people that actually get no --

MS. HARRINGTON: Five seconds.

MR. PATRICK: -- Spam, because they use this. So, put your pens away, just wait a little bit.

MS. HARRINGTON: Ding. Next?

MR. KRAMER: This is an enormous problem; it's been a problem for 10 years and Congress hasn't acted yet. It needs to act now. The problem has reached epidemic levels; the cost of Spam to the industry, to businesses and, ultimately, to consumers, is staggering. This cries out for a legislative solution, and the legislative solution is right in front of us. We already have a model for it -- it's the junk fax statute. Spam raises the same problems as does junk faxes.

We need a legislative solution that allows me, and anyone else who feels aggrieved by a particular

message, to go to court and take action on his or her own behalf, seeking statutory damages, seeking a penalty against the Spammer for its misconduct in such a manner as to vindicate the public interest and to tell Spammers that their messages have consequences; to change the economics of Spam; to put the costs back where they belong, on the Spammers --

MS. HARRINGTON: Five seconds.

MR. KRAMER: -- and get them off of consumers.

MS. HARRINGTON: Excellent, Dave.

(Applause.)

MS. HARRINGTON: You guys are really the masters of the 60-second pitch. Who's next?

MS. SELIS: That's a hard act to follow, but I have to point out that David used to be in radio at one point in his life.

(Group laughter.)

MS. SELIS: He has professional training here. I think the most important thing for the states, and for consumers, is to have effective, substantive enforcement provisions that enable people to go into court and get relief, and that it will ultimately make more sense for a Spammer to stop Spamming than to keep making money.

In other words, I think it's an economic incentive issue. As long as a Spammer can continue to

make money by sending out big volumes -- maybe getting a 1 percent return -- it makes sense for him to keep Spamming. But the minute he has to face criminal penalties, statutory damages, the threat of big lawsuits, he'll stop. It's a dollar-and-cents issue, and if the balance is on the side of fear of enforcement, the Spamming will stop.

MS. HARRINGTON: Excellent, thank you. Who's next? Ray?

MR. EVERETT-CHURCH: I would urge you to resist the temptation to repeat past mistakes, and we've seen mistakes in anti-Spam legislation. Opt-out approaches have not worked; labeling has not worked; and look beyond the borders. Labeling approaches in other countries have not worked. Other countries have moved steadily toward an opt-in approach. Business can live with opt-in -- business lives every day with opt-in -- they do great good and great business by adopting opt-in approaches. The law can encourage companies to do the right thing, to encourage best practices, if the law works to encourage opt-in.

MS. HARRINGTON: Okay. Next? Chuck?

MR. CURRAN: I'll take a shot here. We believe that technology and legislation compliment each other in terms of solutions. There is no magic bullet, and

certainly penalties with teeth for the outlaw Spammers will reduce the incentives and create the kinds of deterrents we think are necessary.

Legislation is also needed, we think, to uphold the integrity of the technologies. The unfortunate history of anti-Spam technology is that it's been circumvented. And, so, legislation, just like in any other kind of criminal activities, needed to back up and set boundaries for activity. Certain technologies can solve a lot of problem and make the experience better, but legislation has to be there to provide the back-up for those who step outside and transgress the boundaries that we've set.

So, we support both approaches and think there is a role for Federal legislation to provide the kind of backstop to a good consumer experience.

MS. HARRINGTON: Okay. We haven't heard from Steve.

MR. RICHTER: Well, I want to say that we can't wait for Enron and WorldCom to hit this industry where we're going to make examples of a few and hope that the others run or then we catch them and we fine them.

This is something that has got to go right now, and my feeling is that legislation has to go, if it's not the best legislation, we can always catch up with it

later. But the EMA absolutely would like to see the Spammers out of business and I agree it's economic, we have got to go after their pocketbooks and that will put them out of business.

MS. HARRINGTON: Okay. I think Jerry, it's to you.

MR. CERASALE: Well, we need legislation. We have to go after the bad actors who are just swamping this internet system, and we have to also open the pocketbook, give money for the Federal enforcers to enforce whatever law you have. That is absolutely required. If you don't do that, don't bother writing a law.

But you also have to keep in mind that the internet is an unbelievable economic and informational system, and you can't -- don't close it up. It's 10 years old, it's still a relatively new technology, in all other channels of marketing; for example, pornographers have come first; and we're still in that stage. Don't close it; let's try and protect it and keep it open so in the future this can be an economic driver for our country and the world economy.

MS. HARRINGTON: Thank you. We're going to go to Commissioner Thompson in just a moment, but speaking only for myself, as a staffer at the FTC, and not on

behalf of the Commissioner or any individual Commissioner, I would say two things to members and Senators: Please make it an offense to send Spam to Commissioner Swindle because he forwards it all to me.

(Group laughter.)

MS. HARRINGTON: So that's my first concern, and the second is on a more serious note, if you do anything that implicates the Federal Trade Commission, please give us the resources to carry out your intent.

Now, Commissioner Thompson?

COMMISSIONER THOMPSON: First of all, I want to thank you all for being here. I thought this was a great panel in hearing from you. But I wanted to maybe sharpen the pencil a little bit, because I heard a range of responses to one topic, and we've talked about whether some Federal response is appropriate and what the nature of that response should be.

I guess I'm a little bit concerned about timing. Have we reached a tipping point, in your eyes, that you think for the Federal Government not to do anything would be inappropriate?

MS. HARRINGTON: Very good question. Panelists? Ray?

MR. EVERETT-CHURCH: If I could just echo what I said at the opening, the Coalition Against Unsolicited

Commercial E-mail has been working on this issue since 1997, when we were founded. We felt that it was a problem then and a growing problem, and that the dire predictions we made and were laughed at for have, unfortunately, come to pass.

So, I'm here to say, we told you so. And a bad solution, a bad legislative solution will only exacerbate the problem. It's past time for a solution.

MS. HARRINGTON: Steve?

MR. RICHTER: Commissioner, I would tell you that it's a disincentive to anybody not wanting to Spam the longer the Government waits to get into this; that the state laws and the precious little that they can do is just not enough; and to me this is a rabbit farm and every single day there's more rabbits, being the Spammers, and there's no reason to tell them to stop proliferating.

MS. HARRINGTON: David?

MR. KRAMER: I think that we've gotten to the point where businesses recognize what a serious problem this is. If we're not in this for the consumers, recognize that businesses are spending hundreds of thousands of dollars to protect the productivity of their enterprises against the onslaught of Spam.

At that point, you know that there's a real

problem here. They're looking for solutions; technology can provide some relief; but legislation can provide more.

MS. HARRINGTON: John?

MR. PATRICK: Well, I think it would be a mistake to take any legislative action, as I've said, and there isn't time to go into all the technology, and I wouldn't attempt to do that, but I can tell you that the technology is working for companies and for individuals. And a lot of the Spam does come through employers and employers are putting technology in their mail servers that are examining the pattern of what's coming in and eliminating huge amounts of it.

MS. HARRINGTON: Okay.

MR. PATRICK: So, technology does work, and we need to give it just a little more time.

MS. HARRINGTON: Okay. The tipping point question, Chuck?

MR. CURRAN: I absolutely think we reached our kind of viral level, critical mass in the last year, and that everyone is now experiencing the sheer load of, as fewer and fewer people respond to any sort of e-mail, the Spammers are just turning up the dial in terms of what is being sent, and that is what is really rippling out, not just the consumerized P level, but at the transport

network level, at the business level, and there really are no impediments to growth other than stronger penalties and decisive action, otherwise there's nothing to stop the growth.

MS. HARRINGTON: Any panelist have anything to add on this tipping question, whom we haven't heard from?

MR. SORKIN: Yeah, I think we're at the tipping point, to mix two or three metaphors, with the bills I see in Congress now, I'm afraid we're going end up on the wrong side of the cow.

(Group laughter.)

MS. HARRINGTON: Moo! Okay. Let's open it. Steve, would you catch this gentleman in the dark blue shirt?

MR. PRINCE: I'm Matthew Prince from On-Spam. Hopefully it's clear that we're on the right side of this debate. I wanted to merge a couple of different issues that came up.

The first is, to start out with the Schumer proposal -- or taking that actually down to the state level -- there are currently eight states considering do-not-e-mail registries on the state level. I was actually just in Michigan the other day speaking with them about the subject.

The second is the state actions and making

state laws effective, and the third is private causes of action. It seems to me that there's an additional benefit of a do-not-e-mail registry that it associates a jurisdiction with an e-mail address. It says that there's a jurisdictional hook onto which a State Attorney General can latch onto a lawsuit, in addition to providing the summary judgments and more effective means of going to court and getting a quick judgment, you can also actually latch on the laws that states are passing, helping solve many of the problems that we're having.

MS. HARRINGTON: What you mean is that there is victim-venued jurisdiction, clearly, in the do-not-Spam laws that help states that may not otherwise be able to effectively assert jurisdiction?

MR. PRINCE: If I have an e-mail address, matthew_prince@hotmail.com, whose jurisdiction applies? Is it Redmond, Washington, where Microsoft is based? Is it Santa Clara, California where Hotmail servers are based? What states are trying to say is their jurisdiction should be able to cover me, a citizen of the state. The problem with e-mail is that it is, at some level, jurisdiction-free, and until you solve that problem, there's going to be no way for a state just to address the issues on a state-by-state-by-state basis.

Furthermore, this actually can extend to the

Federal level. Everyone has said, what is the problem? If I'm a Spammer and I'm sending out mail, how do I know whether an address is in the United States or it's in Canada? That seems like an absolute defense -- and going back to my first year of law school, I mean, that's an impossibility, right?

I don't know what law applies and, then, therefore, there is no way for me to ever comply with the law unless I'm on notice of what I need to comply with.

MS. HARRINGTON: Okay, thanks.

MS. SELIS: You're absolutely right, and I think it's really a state problem more than a Federal problem. In Washington we dealt with that issue by creating a registry, but the state didn't create the registry; the state didn't have the resources to create the registry and our legislature refused to create it legislatively.

So, what happened was an association of internet service providers, The Washington State Internet Service Providers Association, put up an on-line registry so that people could register themselves as Washington State citizens, enabling the state to come in and assert jurisdiction.

So, you point out a very good point and that is that one of the hurdles that states have to jump over is

that jurisdictional one, which is yet another reason why there should be Federal legislation.

MS. HARRINGTON: Okay. Sheryl, let's go to the gentleman back with the glasses and the shirt and tie. To that handsome devil in the back row. It's hard to describe people in the audience from up here without offending.

UNIDENTIFIED SPEAKER: First of all to John, I would make a brief comment, which is, I spent the last year and a half working on anti-Spam filtering technology and more recently corresponding with a lot of the people throughout the industry who are working on the technology, and they are not nearly as confident as you are. I think everyone who is working on the technology feels severely the limits of what can be done by technology alone. And there are many of them here today in the audience who'll be happy to talk to you.

(Group laughter.)

UNIDENTIFIED SPEAKER: The second point, I have a question for the panel which is, as I understand it, and this is very new legislation, Senator Schumer's bill goes quite a bit beyond the do-not-Spam registry that everyone has latched onto and, in fact, covers a number of other areas relating to Spam, including some of the falsification of trespass on servers and some of these

other issues. I'm not yet aware of all the details, but I wonder if any of you could comment on those provisions of Senator Schumer's bill.

MS. HARRINGTON: Well, I think Senator Schumer indicated when he was here that he hasn't introduced his bill and that he has a number of ideas that he intends to put forward in the next couple of weeks; and, so, I think that beyond the do-not-Spam registry idea, for myself, at least, I haven't seen the proposals and it's hard to comment.

I don't know if anybody on the panel has seen any additional language or proposal from the Senator. Anyone? Anyone?

(No response.)

MS. HARRINGTON: Okay. Too soon. Steve, can we go to the woman in blue in the back? Aqua? Turquoise?

MS. COHN: I have to ask my mother, she picked it out. This is Cindy Cohn, I'm with the Electronic Frontier Foundation and I wanted to just make a comment on something that Brian said and make sure I understood him.

MS. HARRINGTON: My Brian -- our Brian from the FTC?

MS. COHN: Yeah. Brian asked whether we needed

positive identification capabilities for noncommercial as well as commercial e-mail, and --

MS. HARRINGTON: No.

MS. COHN: Did I misunderstand?

MS. HARRINGTON: Yes.

MS. COHN: I think it's really important that we make sure that in these laws that we recognize that a lot more goes on in the internet than commerce.

MS. HARRINGTON: Yeah, but Brian's distinction was unsolicited/solicited. So --

MS. COHN: Oh, I misunderstood?

MS. HARRINGTON: Yeah. We're only talking -- I believe -- Brian, am I on your wavelength?

MR. CERASALE: My answer was only on commercial.

MS. HARRINGTON: Yeah, okay. Moving along. Sheryl, the guy with the blue shirt-sleeve right there. Vince -- you're not Vince, but that's fine.

MR. BLACKMAN: My name is Ed Blackman from Eureka Computing Solutions, and I want to agree with John. I don't think there is any legislative body with global authority to regulate e-mail. What we need is a market-based solution. Sending Spam has to cost the same as printing and sending bulk mail, and until that happens, we're going to get inundated with Spam.

MS. HARRINGTON: Okay, so it's the cost shifting issue?

MR. BLACKMAN: It's a market-based issue.

MS. HARRINGTON: Okay, thank you. Steve, the gentleman in the front row up here in the tan.

MR. HENDRICKS: Yeah, thank you. Evan Hendricks, Privacy Times. It seems to me that, you know, why do they rob banks, because that's where the money is; why do they send Spam, because that's where they're trying to make money. The experience shows we have a significant percentage of people who are in the United States of America that are Spamming, okay?

So, our laws have never been designed to stop crime around the world or to regulate it around the world, but if a U.S. law can help stop the problem in the United States and bring people to justice or create economic penalties, I don't understand how you can be against a U.S. law, John, that can cut into a significant portion of the problem.

MS. HARRINGTON: Well, what a nice set-up for the next panel, which is going to deal with the international aspects, and I think that's a bit rhetorical, so we're going to move on.

Back here, in the blue shirt -- Steve or Sheryl or someone. That's okay. This is likely, I think, to be

our last audience question.

MR. SWILLINGER: Mark Swillinger from the law firm of Sonschein, Nath and Rosenthal. I just wanted to follow up on the question David raised about businesses.

My clients, corporate America, is concerned and is spending money on fighting Spam and they want to know why none of the state proposals or Federal proposals deals with a corporation's ability to control its own network. That is, if a corporation says, I have 100,000 e-mail addresses around the world, you can't send e-mail to any of them, if it's commercial Spam, why shouldn't that trump an individual employee who signs up for a list and says send me messages?

MR. KRAMER: Interesting question. I suspect that -- let me answer it this way first, to say that California's law, Business and Professions Code 17538.45, takes exactly that approach to the problem. I happen to know a little bit about that statute.

(Group laughter.)

MR. KRAMER: It basically says you, as a business, have the right to control who has access to your mail servers, as long as they're physically located in the State of California, and you can give notice to whomever you choose that their messages are not welcome on your network. So, it's not quite accurate to say that

that hasn't been discussed in the state legislative efforts.

I think that the problem with California's approach is that it's a state's approach, and at the state level -- I touched on this before -- the state needs to be quite careful about how it goes out and tries to regulate interstate commerce.

So, a state that, for example, said, you cannot send messages to any businesses in our state, would have some problems because as Jerry and others have pointed out, a Spammer doesn't know where his or her messages are going. So, California has this rather cumbersome process that says, hey, you have to give notice first that your messages are going to be using servers that are located in California before you can sue, and if we had that at the Federal level, I think it might be a useful, but certainly not, end-all solution to the problem.

MR. EVERETT-CHURCH: If I could say this real quick, that that statute in California does also include something very useful. It says that, if technology comes up with a better way to provide notice in the future, that that notice can be effective, rather than certified mail and service a process, and the Coalition Against Unsolicited Commercial E-mail has proposed, at the Federal level and in state legislative proposals as well,

to create a standard to work through the technical standard's process for the internet, to encourage a technical standard that could be recognized in statute and enforced, that would give recipients the ability to say, we don't accept unsolicited commercial e-mail. And there are technologies that could make even more granular statements possible. We don't accept certain types of unsolicited commercial e-mail, adult e-mail, et cetera.

MS. HARRINGTON: Okay. We're almost out of time. We began with Commissioner Swindle. I think, Commissioner, you may have been out of the room when I made my plea to Congress if they legislated at all to prohibit Spam to you since you forwarded it all to me, and also your friends. We want their Spam blocked.

(Group laughter.)

MS. HARRINGTON: Is there anything that you would like to say, as we wrap up this panel?

COMMISSIONER SWINDLE: Solve the problem.

MS. HARRINGTON: Solve the problem.

COMMISSIONER SWINDLE: You know, we spent, what, two hours here discussing, in very complex terms a very complex matter, and that is legislation and law and how we can deal with this. I still go back to my concern for consumers. Will somebody that has more brain power than me, come up with a way to give the consumer the

power to say, no -- period. That would solve an immediate problem for an extended period of time.

The guys are going to try to get around that and they will get around it, but in the meantime we've diminished the frustration of consumers. And, as I said, if this frustration gets to a high enough level, we have done some irreparable damage, and we need to solve that.

So, I would challenge AOL and Yahoo and Microsoft and Earthlink and on and on and on to start competing with each to give consumers the power to say no. And the one that comes out of the shoot first is going to be a big winner.

Thank you.

MS. HARRINGTON: Okay. Well, we're going to wrap this panel. In 10 minutes we will begin with the international panel and we will start promptly.

Thank you, panelists.

(Applause.)

(Whereupon, a brief recess was taken.)

MR. STEVENSON: All right. I'm Hugh Stevenson from the Federal Trade Commission and we proceed now to the Panel on International Perspectives on Spam. And I think we heard right from the start of this forum about the importance of considering Spam from an international perspective, and this has been an issue, and not

surprisingly, of concern to many countries and, so, we're able to assemble really a truly distinguished and diverse panel of foreign visitors to offer their views here. We really appreciate their taking the time and trouble to come from so far away to offer their views.

And I think that it's important to emphasize that getting their views is important, both so we can compare notes -- what has their experience been with Spam; what has their experience been in terms of legislation; what challenges have they seen in trying to enforce the legislation they have.

It is also an important issue because, as I think a number of people have noted, enforcement is a global challenge, as well, requiring international coordination and cooperation. And that requires thinking about how do the various national approaches there fit together.

Our format for this panel is that we've asked our speakers to start by giving a five-minute introduction, talking about the experiences they've had in their countries, and we will then turn to a discussion format and take questions from the audience, if people have them.

I'd like to start in Asia. There is some legislation already in place in Korea and Japan, and

we'll turn first to Dr. Hyu-Bong Chung from KISA, which is the Korea Information Security Agency. KISA has done, actually, a paper that is out on the tables out there on the Spam laws that they have, which date back, I think, initially to the year 2001, and I'd also note, they have collected an increasing number of Spam complaints. I believe they had over 100,000 for the year 2002.

And, so, Dr. Chung, I turn it to you.

DR. CHUNG: Thank you. Thank you, Mr. Stevenson. Good morning. I am from Korea, but definitely from South Korea, not from North Korea.

(Group laughter.)

DR. CHUNG: As we have discussed two-and-a-half days, there are lots of policy measures and options of alternatives we have at our hand. I think, personally, that we can briefly categorize those tools into three. One might be legal approach and the second might be technical approach and the third would be, I think, market approach. When I say, market approach, it means pricing scheme and so on, which we can think about.

Okay, since I have a very limited time, I will just focus on the legal approaches which we have pursued over two-and-a-half years in Korea. So, let me first start with some background information; some numbers, which gives you some understanding of the current

situation in Korea.

Total population of Korea last year was around 47 million, and about 58 percent of the population, which is equivalent to 26 million, reports that they have access to the internet and use it at least 12 hours a week. And we have, also, around 30 million people who use mobile telephone, hand phone sets.

Eighty-five percent of internet users in Korea, around 22 million, report that they have e-mail accounts and almost every individual and business owns -- uses e-mail address and enjoys this powerful medium for expressing ideas, sharing information and opinions and doing businesses.

The result of a survey of 2,000 e-mail users conducted by KISA last year shows that every user has an average of four e-mail accounts and receives 14 e-mails every day in each account. And eight out of 14, they report, were unsolicited and unwanted ones. So, around 60 percent is unwanted ones. This is a rapid increase from 2001 when Spam occupied 44 percent.

Fifty-one percent of respondents replied that they do not even read and they just delete it immediately upon their receipt and only 40 percent reported they read the ones only with interesting titles.

Next, let me move to the regulatory efforts of

the Korean Government to control the Spam. Anti-Spam legislation in Korea has been enacted since 1999. The law prohibits the transmission of unsolicited commercial e-mails. The regulation has evolved to become stricter over time, as the prevalence of Spam increases in the market.

In Korea, sending commercial advertisement information against the addressee's specific rejection is illegal and subject to penalty. In addition, under the law, the sender of commercial advertisement should identify the name of the sender, e-mail address and the mailing address to contact and provide convenience for said recipients to express their rejection of the e-mails.

Despite this regulatory item, the Spam increased rapidly on the internet and we introduced new regulation to help to ease the Spam filtering by recipients.

From July last year, the senders of commercial advertisement are required to include labels about the advertisement specified by the law, such as advertisement or adult advertisement in Korean and English in the title of their commercial e-mails. A breach of this requirement is subject to fine under the law.

To fight against the technological development

of Spamming, we also introduced several regulations, from January this year. First, we added unsolicited messages via telephone and other media for the definition of illegal Spam, including wireless mobile phones.

Second, sending advertisement implying media materials harmful to minors. For example, obscene and violent ones to the minors is prohibited. That is subject to the criminal sanction.

Third, automatic harvest of e-mail addresses from the website and the other internet is prohibited.

Last to the technical manipulation to evade the law and avoid the recipient's refusal, automatic generation of a contact, such as e-mail addresses and telephone numbers, is prohibited by law.

For the details of the regulations I mentioned, I want you to refer to the handout that reads, Anti-Spam Regulations in Korea.

To enforce the laws to control the Spam, KISA, for which I am working, established Spam Response Center last year, and in 2001, we had 254 complaints against Spam from the public, and last year we received 69,609 complaints, literally an explosive increase we had. In the first quarter of this year, we received 27,810 complaints.

Besides the enforcement laws, KISA also

conducts public awareness programs and technology development. We opened a website to provide information to reduce the suffering of the public last year. We provided useful information for filtering unwanted e-mails for the end users of the e-mail services and tips to avoid receiving Spam.

We also inspected the 40,000 mail servers in the country and provided technical assistance to block the Spam relays. KISA also developed a special software to protect the websites from automatic e-mail address harvesting and made it available to the public from our website.

We organized, also, a coalition network fighting against Spam with mail service providers and ISPs in Korea and we established hotlines between KISA and mail service providers. Korean ISPs and mail service providers are becoming more and more proactive in fighting against Spam and protecting their customers. To save my time, I will not elaborate about that.

Let me just speak about my our concerns, lastly, at the international level. We have found more and more Korean Spammers are moving out of Korea and into foreign countries, such as the U.S., to avoid punishment of the law. For example, illegal pornographic e-mails are under strict control by Korean law. The Spammers

moved their mail servers and pornographic web service to a foreign country and they operate there.

The second thing I want to mention is actually a suggestion. I suggest choosing and using a common international symbolic letter for the labeling of commercial advertisement e-mails. As I mentioned before, we have mandatory labeling law, but it requires putting Korean letters -- Korean language -- and does not work for American recipients, since no U.S. citizens understand Korean letters. Similarly, commercial e-mails from U.S. sometimes has the label, ADV. That will not work for Korean recipients because they do not understand English.

In conclusion, I wish to emphasize the need for close international cooperation, especially among the policymakers and the interested parties in each country to reduce the Spam. I think this is one of the most urgent issues for us to improve the internet use environment at the global level in these days.

Thank you.

(Applause.)

MR. STEVENSON: Thank you, Dr. Chung. We'll turn now to Japan, which also has passed recently some legislation on Spam. We heard a little bit about it yesterday from the representative from NTT DoCoMo. We

have now Mr. Motohiro Tsuchiya, who also -- I actually should invite our panelists, if they want to, to just sit down and talk would be fine to, so we don't have to walk around.

So, Mr. Tsuchiya, if you want to describe the Japanese experience.

MR. TSUCHIYA: Thank you very much. There used to be a big trade gap between the United States and Japan in terms of automobiles or a semiconductor or everything, but we are now importing more Spam from the United States, so. . .

(Group laughter.)

MR. TSUCHIYA: Now, we are actually learning what American culture is through Spam, so. . .

(Group laughter.)

MR. TSUCHIYA: My colleague is always forwarding his Spams, and isn't it interesting. And I just say, just throw away, but he is always forwarding it.

We have a kind of similar regulation with the State of California, but it's working in Japan. So, somebody -- as the last panel said, labeling is not working in other countries, but it's working in Japan.

I have a one-page handout for the entrants. But I came late, so everyone does not have this, but I

have a handout, so please look at it.

So, I don't want to repeat regulation legislation in Japan, as Mr. Murayama told you yesterday, but there are two laws: One is regulating advertisement owners; the other one is regulating Spam senders. So, the content of the legislation is almost the same. So, you have to put a kind of ADV sign, written in Japanese, in the header section, and you have to give your real name and physical address and no fake e-mail address and never send again to the customer who opted-out.

Ministry can issue an order, so you should stop this Spam or something like that. After this, they can punish the sender or advertisement owners. So, their penalty could be two years in prison or $25,000 U.S. a fine, or a company can be punished. The fine will be -- oh, I am sorry, it's a big number, $3.5 million U.S. a fine. So, this is working.

I have a number. The first quarter of the last year, there were 173,000 complaints about wireless Spam. But one year later, only 74,000 complaints. So, almost less than half. So, it's working. It's not perfect yet, but it's working. It's reducing the number of Spams.

And why are these regulations effective in Japan? I have no clear answer about this. There are several reasons. One is cultural difference. So,

Spammers don't want to take any risk to do legal attempts and online shopping and credit card shopping is not popular -- less popular than the United States, so they don't want to buy online. So, they just want to go to shops.

And maybe the second reason is social sanction. So, if Spammers are penalized or publicized, family sanction or community sanction is more stricter than in the United States. So, we are living in a small country and we have many day-to-day communications.

And the third reason will be the stricter domain name legislation. So, Japanese country is .JP and JP NIC (phonetic) institution is regulating the JP NIC domain names, and they request more detailed information of the owners of the domain names. So, they can easily identify who is owning this domain name and who is used for relaying Spams.

The last reason should be ISP control. So, a judicial precedent allows an ISP to stop Spams in terms of wireless Spam. So, all Spams that go to wireless phones or mobile phones goes through the NTT DoCoMo servers or the KDDI servers or a J-Phone (phonetic) server. So, if ISP finds this is a Spam, they can stop. Of course, Spammers cannot appeal, but they can go to a court. They can fight in the court. So, this is allowed

for the ISP to stop Spam. This reason is very possible, but this is not perfect. So, this is our experience. Thank you very much.

MR. STEVENSON: Have you seen a mix in terms of a change in terms of the amount that appears to be from outside Japan of Spam?

MR. TSUCHIYA: Mostly from --

MR. STEVENSON: You spoke of the imported American culture and --

MR. TSUCHIYA: Yeah. Actually, there's no official stats, but somebody -- interested people are counting the numbers of Spams. They said -- people are, on average, getting 10 to 30 Spams per month and maybe 80 percent or 70 percent from outside of Japan. So, Spam written in the Japanese language is decreasing.

MR. STEVENSON: So, those other ones, a lot of them are in English then?

MR. TSUCHIYA: English, Chinese and Korean, but mostly English.

MR. STEVENSON: Okay, thank you. Well, why don't we turn next to Australia and Canada. These are countries that have privacy legislation, but not Spam-specific legislation at this point. Our first Australian speaker is Tom Dale who comes from -- it's called NOIE, the National Office for the Information Economy of the

Australia Government, and they last year issued an interim report, and last month a final report, on the issue of what to do about Spam.

MR. DALE: Thank you, good morning. Yes, the agency that I represent is an Australian Federal Government agency, the National Office for the Information Economy and about 12 months ago, the Federal Government in Australia asked us to conduct an inquiry into Spam for essentially the same sorts of public policy reasons that you've heard elaborated on in great detail here over the last couple of days. We published, as Hugh said, a final report only a week or two ago. It's available on our website, the ever popular www.noie -- N-O-I-E -- .gov.au in the equally popular PDF format amongst others, so help yourself.

At any given time, I guess, there are no end of reports from government agencies floating around the system in most countries. In this case, however, we found as an issue of public policy that Spam and the need for some measures, including government action against Spam, has a great degree of political support across the political spectrum and we're hopeful that the measures that we've recommended will be adopted by the government, and we've had some indications from our minister already that the government will be proceeding as quickly as

possible on most, if not all, of those recommendations.

There are basically three sets of actions that we're proposing to address Spam issues in Australia coming out of our report. Those dealing with legislation -- and I'll talk about those because that's been a topic of much interest this morning, of course. A number dealing with joint action by government and industry, and Mr. Coroneos, on my right here, is from a major Australian internet industry body and he'll be talking about the complimentary industry initiatives that we hope to go forward with there.

And thirdly, and very important for this morning's session, I think a number of international perspectives on the issue. I don't quite know why Tajikistan was singled out this morning for particular attention, but I have nothing against them one way or the other. I do know that, like Japan, we're finding, as far as Spam is concerned, Australian e-mail users are finding out far more about American culture than they really wanted to know.

(Group laughter.)

MR. DALE: However, let's talk quickly about legislation firstly and what we think will be an appropriate set of legal measures at the Federal Government level in Australia, and I should stress that

Australia is a federal system and at the moment, as Hugh said, there is no Spam-specific legislation at either the federal or the state level in our country. There is federal privacy legislation, which has recently been extended to most of the private sector. But its application to Spam as Spam, putting the content issues aside for the moment, isn't really clear at the moment.

So, what we concluded in our report was that there was a need for federal legislation which would have the following features. Firstly, that no commercial electronic messaging should be sent without the prior consent of the end user unless there is an existing business customer relationship. Now, is that an opt-in screen that's being proposed? Yes, it is.

Before I go on, I should stress, we're very careful to use the term "electronic messaging" because we believe that for purposes of government policy, we have to encompass not just e-mail, which is where the majority of the problems are at the moment, but emerging problems in areas like real-line chat or instant messaging, heaven help us, and also wireless or SMS Spam potential problems. We believe that we can address those as part of the general package of measures here.

Secondly, we believe legislation should provide for all commercial electronic messaging to contain

accurate details of the sender's name and physical and electronic addresses. Now, I think we're familiar with the reasons for that, again, through discussions here over the last few days, and there's nothing particularly unique about our reasons for wanting that.

Thirdly, we are suggesting that there be provision in the legislation for what we term in Australia a "co-regulatory approach" with industry, which provides, if you like, a regulatory incentive for industries to develop codes of practice to address issues so that the legislation does not have to be called into play, but there is provision for enforcement of the legislation should the industry be unable to apply or agree on codes of practice, and that has worked quite successfully in a number of other areas of internet regulation in Australia and, again, Mr. Coroneos has been an active participant on the industry side in that kind of regulatory approach.

And, finally, we'll be including in that legislation, should it go ahead, appropriate enforcement sanctions which would include, probably at the least, a range of criminal sanctions and we're certainly looking closely at the issue of scope for private action, as well, again covering some of the broader legal conceptual issues covered in the panel session earlier this morning.

MR. STEVENSON: What has been the reaction to your legislative proposals in Australia?

MR. DALE: Generally very supportive from most industry areas and also from a number of internet user groups and political parties, as well. The only qualification -- and it's not a major one and perhaps is not a surprise -- is the Australian Direct Marketing Association had some concerns and we believe that we'll be able to work through the concerns of the direct marketers through perhaps some code of practice issues or focusing on that prior existing business relationship provision that I talked about.

So, generally, it's been pretty hard in the last couple of weeks since the report was released to find anybody who has a major problem with it, which is pretty encouraging for any area of public policy.

MR. STEVENSON: Great, well, thank you. We'll turn now to Peter Coroneos, also from Australia, the Chief Executive of the Internet Industry Association, and the IIAA just last month announced an industry initiative to address Spam and if you can describe what that's about and also what industry reaction has been to the NOEI initiatives.

MR. CORONEOS: Thank you, Hugh. Firstly, I'd like to thank the Federal Trade Commission for inviting

me to attend this session, and particularly to Commissioners Mozelle Thompson and Orson Swindle, both of whom I've worked with personally on issues ranging from privacy to security and consumer protection. And, in fact, we see Spam as covering all of those areas, so I think it's highly relevant that whatever initiatives and international cooperation we can put in place, perhaps as a result of this forum, will also have, hopefully, a positive contribution to make in those other areas as well.

What I'm going to say might seem shocking to you when I describe to you who our association is and who we represent in Australia. As Tom said, we're the national industry body for the internet. We have over 300 companies, representing a Who's Who of the internet industry in Australia. They include players like Telstrel (phonetic) Optus, AOL, Aussie Mail, MSN, Yahoo, a lot of the major security and filter providers, Symantec, GenMicro, Message Labs, and others, and, of course, several hundred smaller players as well.

One thing is clear and one thing that our members all agree on, however, is that Spam is killing the Internet. We are seriously concerned about the undermining of the essential utility of e-mail, and as Commissioner Swindle said today, that remains the killer

application in Australia and the rates of Spam that we are now experiencing in Australia are equal to those that are being experienced elsewhere.

So, this is no longer a matter of choice for the industry. This is really, at the point now, one of commercial necessity where we have to act in the interests of end users if we are to preserve the rates of growth that we've been experiencing in the past. And, interestingly, I was in Washington this week when AOL, Microsoft and Yahoo jointly announced their combined initiative to combat the Spam problem, and I think that, in itself, is highly significant, given that our U.S. affiliate in Washington has informed me in the past how hard he's found it to get competitors to work together.

The fact that we now have competitors all pushing in the same direction here is evidence enough of the seriousness of the problem.

To that end, in Australia, we launched what we believe, two weeks ago, is a world first in terms of industry proactive response or industry proactivity to the question of Spam. And there's a press release outside on the table that describes what we've done, but essentially, we are providing for the next month, starting from about two weeks ago, every Australian internet user, be they corporate, small business or home

user, with a free internet Spam filter for one month, and after that, there are very low cost plans. In some cases, they'll remain free. Because we believe that there are technical solutions out there that are capable of empowering people to take control.

We acknowledge that they're not perfect solutions. We also acknowledge that legislation is not going to be perfect either. But we believe that if we can do what we can as an industry, and remembering that our members touch collectively over 80 percent of every internet user in Australia, we think that is an incredibly powerful statement to make, and I have to tell you that the URL for this, if you'd like to write this down, is www.iia.net.au/nospam. If you go to that page, you'll see the initiative and you'll see the 11 vendors, all fierce competitors in the marketplace, have all come together under this initiative, because we're trying to raise awareness as to the availability of the solutions and also to encourage them to use it.

I know I'm running out of time here. I just wanted to say one quick thing about legislation because I know that that was a part of what I was asked to address. Our industry association is not opposed to legislation provided that it's effective legislation. One concern that we have is that opt-out legislation, which creates a

very low threshold, is not going to be effective.

And the major point -- and I'm happy to talk about this later -- is how does a so-called legitimate e-mail marketer differentiate themselves from the worst kind of Spamster, and I think opt-out is problematic in that it's too easy for the wrong kind of players to comply with that and you end up with a solution where, you know, the aggregate effect of me getting 30, 40, 50, 100 opt-out e-mails in my mailbox every day still constitutes a Spam problem of major proportions.

So, we can talk about that, but that's our perspective as the industry in Australia. Thank you.

(Applause.)

MR. STEVENSON: All right, we'll turn next to Peter Ferguson -- from Peter Coroneos to Peter Ferguson who is from Industry Canada, who's long been involved in privacy issues. And Industry Canada, I believe, put out a discussion paper on Spam back in '99 and is now having a process of consulting with its stakeholders and revisiting the issues that were addressed then.

MR. FERGUSON: Thank you very much, Hugh. Let me update you very quickly on what's going on. I'd like to offer some comments generally about international cooperation at the conclusion. Our policy on Spam, our current policy, was developed in 1999 and it basically

takes the position that the application of existing laws, appropriate industry policies, technology, and consumer awareness can, to a large extent, curtail e-mail abuse.

We have been subject to criticism over the last year about that general thrust, most of which is focused on the fact that the burden really is shifted to the individual consumer, and it's true in terms of actions that need to be taken and cost. However, the policy is consistent with our general approach to the internet, which is one very much of hands-off.

Laws of general application do apply in Canada. Particularly, there are provisions in the Criminal Code of Canada that can be applied to the Spam situation. However, I should note that the Criminal Code is a federal act. The problem is that it's enforced by the provinces and the response from the provinces is, I think to be polite about it, uneven. And I think it's uneven generally towards the e-environment. It's not just the matter of Spam and that really does get us back to a serious resource question that we've got in Canada about enforcement of the Criminal Code.

By the way, we do have Spammers in Canada. I don't say that with pride. We don't have any sense of volume, but they are there.

We began the current review in 2002 more in

response to media pressure than to individual complaints. Unfortunately, my name is at the bottom of the current policy. So, my phone does ring and that does sharpen my attention, and it has contributed to us getting on with the particular review.

We put a discussion paper out in January of this year. We sent it electronically to 19 key stakeholders and I think it's fair to say that within 24 hours it was everywhere.

The paper focuses on seven specific issues, consumer choice, filtering technologies, their effectiveness, are they part of the premium or basic service, appropriate industry policies, what might those be, network solutions, what might some of those be, a role for government, are new laws required, applying existing laws, Spams and scams, and the question, of course, of enforcement, and consumer awareness, who has the lead responsibility with respect to consumer awareness.

Very quickly, some of the responses, consumers consider Spam filtering a part of basic e-mail service and most put the responsibility on ISPs to clean up the situation. Most internet users, when we asked the question, are not comfortable with desktop filtering. There's a consensus in all of the responses that there is

no silver bullet and that a tool kit approach is necessary. Industry does not see a need for new law, but better enforcement. Consumers see a need for new law. So, we've got a polarization around that issue.

If we are to consider legislation, I would note that it would have to be based on good public policy if it's to be effective. So, we're really moving ahead now on the tool kit strategy. We want to set long and medium term targets. We want to allocate responsibilities and get agreement on what those would be in the marketplace and to identify common initiatives. I won't, because of time, go into what some of those might be, and it is very much, at this point in time, might be.

Next steps for us is then going to be convening key stakeholders again on a common approach in the development of what we hope will be good public policy and we hope to have a meeting in June of his year, taking advantage of this workshop and also one being hosted by the ILPF and Global Business Dialogue on Electronic Commerce in June where Spam is one of the agenda items.

We want to have a practical action plan and I want to stress that. We've really got to be able to do some things and do them now. But -- and this is where I want to really bring in the need for international cooperation. This is not a subject, as we've heard this

morning, that's going to be handled in splendid isolation. We need to bring to the table internationally good domestic policy. The stronger the domestic policy is, the easier it's going to be to arrive at useful solutions.

We want to avoid the away syndrome. I think certainly in Canada, but we have to do it internationally. Driving Spamming offshore and creating safe havens is really no solution for anybody.

We want to look at Spam in a broader context and I really think we have to do that. We've heard allusions to security of systems and networks and I think we've got to pay much, much more attention to that. And we do have, from an OECD perspective, the OECD security guidelines, which we spent an immense amount of time updating over the last two years, and a real push, we think, is needed in the private sector to become much more conscious, aware of and active in implementing appropriate security measures for this environment.

I think another thing that needs to be looked at is the whole question of the economics of the Internet and probably an organization like the OECD would be a useful body for international cooperation to better understanding how the economics work and how we might address some of those problems of, for instance, passing

costs onto consumers.

The OECD is 30 member countries. There are three working groups, at present, tasked with looking at the Spam issue, a technology policy group, a consumer policy group and the group I'm part of, Information Security and Privacy, and we are cooperating and moving ahead on work.

What's missing from this equation is involvement by APEC, the Asian Pacific Economic Cooperation Forum, and I think we really have to drive APEC into formal discussions on that, internally and in cooperation with the OECD. And, finally, let me note that I think our international work really has to focus on the doable, on harms and on vehicles for mutual recognition and mutual cooperation, and that's a big task, but I think it really does have to be addressed. I'll stop there.

MR. STEVENSON: Thank you very much. We'll turn now to Europe where there are more extensive regulations that have been in place to address some of these issues. And our next speaker is Philippe Gerard from the European Commission. The European Union has a directive on electronics communication privacy which was -- that dates from, I believe, last year, and this is a directive that, even as we speak, a number of the members

states are working on implementing and so, Philippe.

MR. GERARD: Well, thank you. Thank you, also, for inviting the European Commission here today. It's a good thing because it is a global issue, so I think it's understandable that we look at what's going on in other parts of the world.

It's been a very interesting workshop so far. I didn't travel just for two hours, so I've been here for a few days listening to what people have said and, in fact, I've never been more convinced than today that we may have chosen the right solution, i.e., an opt-in solution.

Well, probably I need to give you some background information on how things are regulated in the EU on privacy first of all. We have a horizontal data protection directive which is applicable to both public and private entities, and that includes general principles on how, for instance, you can process personal data. This is important to bear in mind because this may explain why so far harvesting, for instance, has been less of a problem in Europe compared to the United States, simply because you can't pick up lists wherever you want and start e-mailing people. So, that's an important part of the answer probably to Spam.

Now, we have, also, an inter-market principle,

that means that within the EU, if there's an obstacle to the freedom to provide services, we can take legislation. It's a bit like the interstate thing here. And so, we have had the Telecom Data Protective Directive in '97 where we provided for an opt-in for faxes. Well, this was in '97. Then we had in '99, the review of the entire set of laws for telecommunications, which we call now electronic communications because we don't want to take different approaches, you know, depending on whether you send mobile communications or e-mails or fixed communications, et cetera.

So, we tried to design a technologically neutral approach and that's why in terms of the -- and so this is a commercial communications and we have now an opt-in system which is applicable to faxes, to e-mails. And when I am talking about e-mails, I'm talking about electronic mail as we know through the internet or SMSs or MMSs. It's all the same answer, if you want, because there's no reason to differentiate we think.

Of course, it's been a quite tough debate, as you can imagine. There's been strong lobbying. People around the table will not agree. But I think we've found a good solution because we think, first of all, we've provided user empowerment. That's, I think, a key element here. We keep talking about consumers. In fact,

there's an easy way to tackle this which is to leave it to consumers to say whether they want or not electronic commercial e-mails. That's one element.

And, also, in terms of marketing, and that's what was important for us, we really think that permission-based marketing is more efficient. So, we see no sign that sending e-mails to thousands or millions of people is very efficient in terms of marketing. So, we really think that permission marketing is more efficient. So, there's no reason to be afraid of an opt-in system. That was our conclusion.

So, let's talk probably about now the opt-in system in greater detail. Well, what does it mean, opt-in for e-mails? It means that the use of e-mail for direct marketing to consumers is only allowed when subscribers have given their prior consent. Actually, it's kind of an easy definition. I'm not saying that it will be easy to implement in all member states, but at least the principle is easy to understand.

As I said, e-mail means SMS, MMS, et cetera, it must be for marketing purposes, so there's no question of preventing normal communications or non-commercial communications. We're talking about marketing.

Well, the advantage of this system is that you don't have to enter into discussions about what is bulk

or what is not bulk, what is Spam or not Spam, what is deceptive, not deceptive, what is fraudulent and not fraudulent. You have to say, did you get the consent or not. Then you can start your marketing practice.

Well, there's an exception to this opt-in system which is when you have an existing customer relationship. Again, you have to see this in the context of purpose limitation and are the rules applicable. So, it's not like if you had once a contact with someone just through a website, you cannot take advantage of this to Spam that person. You have to control that -- I mean, to start from an existing sale or the context of a sale as a minimum.

Also, it's business to consumers, right? Business to business is left to member states, individual member states to regulate. This means that they can choose. But, of course, you can choose to implement an opt-in for business to business, also. That's easier.

Also, we've got kind of additional safeguards, like the disclosure of the identity of the sender, which is required. And you have to have a valid opt-out address in there. So, we've got probably the entire set of measures, at a logistical level of course. In terms of enforcement, of course, it's for member states, individual member states to enforce that. It's not for

the Commission to do that.

We can coordinate, we can promote, we have a provision saying that there must be enforcement, there must be a right of action, but what you would probably call private right of action. There must be possibly to claim for damages and there must be suitable damages to ensure effective implementation at member states' level and there must be sanctions. So, this is also a kind of diverse set of enforcement tools.

On implementation, well, we have conducted a consultation with member states, with data protection authorities or agencies if you want and to see what practical follow-up we could take in terms of not only legislative action, but also awareness raising activities, contacts with the industry to see what a possible -- like codes of conducts could be adopted, et cetera. We're still in the process of deciding on this follow-up, so I can't tell you more about this. Probably we'll come back to international cooperation later on.

MR. STEVENSON: If I can ask you just one follow-up question. What are the main concerns -- because you're in the process of the member states, the countries in the European Union -- transposing this or implementing it in their own laws? What are the main concerns that they have raised? If I have the timing

right, that process is going on now.

MR. GERARD: Well, I would say it's nothing unusual, right? When you draft legislation in an individual member state, you get questions of interpretation, right? What does this mean? What the opt-in means -- what the opt-out means for an existing customer relationship? We have limitations. When you have this opt-out, it must be for similar products only and by the same legal entity. So, you can imagine the kind of forceful lobbying to understand what it is in whatever direction. But this is the kind of thing that we have at the moment.

MR. STEVENSON: Thank you. We'll turn now to Marie Georges from France's Privacy Protection Authority. Last year, her agency did a very interesting study on Spam. They set up a Spam box and received, I think, over 300,000 Spam and there have been copies out on the table of this report. And France also has some law that, I believe, predates the directive that has been used to address these issues. So, we thought we'd benefit from hearing from the French perspective on this, as long as there are no comments about exportive U.S. culture.

(Group laughter.)

MS. GEORGES: Thank you. I could be up, but it is not necessary. Just to show our logo, just because

it's quite an international one with the French (speaking French), better show the European one and democracy as a figure of Greece and the digitalized democracy which is not so nice. If you can show it, that's all. But you can stop it now.

I would like just to add to what Philippe just said that in the European model, as you know, the enforcement is both at the level of independent data protection authority and a court. The authority I belong to, the Board is from the ways people elected from the Parliament, both Senate and House and Congress. Also, high churches, and there are 17 and I'm in the staff.

I would like to say that regarding Spam as we have been set up in '98 and with experience in both public and private sector. We have, by the way, a priori control upon the public sector. No public file can be set up without our favorable, positive opinion.

We have, also, investigation power. But we don't have sanction power for the moment. We may have with the new law this year. But what we have, also, as a mission is to follow new practices, new technology and I would be a testimony of the fact that it's not because you have general laws with general fair information principle coming from the United States. In our European laws, it prevents the progress of technology, but it

gives because they are neutrally technically like fair collective principle, like purpose principle. I don't see technology in that, but it is very coherent with technology -- with that technology.

So, it gives us the mean to follow the practice and react currently. For instance, the question of Spam came up -- well, by '97 or so, not -- I mean, several practices at that moment, mainly list serve mailing lists were attacked. So, we worked with these people to see how to settle the problem. Then, because we are well-known in France, people who wanted to start to make software to grab information in the public space came to us and said, well, how can I do that. We'd say, well, I'm sorry, even if you have -- it's a hard time for you because of the economic situation, but I think it will be prohibited and things like that.

We made a lot of educational programs with also professions, and I can say that all the recommendations that we took in '98, '99 were in the code of conduct of professionals at that time, we have been very much discussing.

We didn't have the opportunity at that moment, but we had already information at the time of collection and possibility to object right away by a box you check at that moment. Any time you collect data for any kind

of purpose, for another purpose than the one who is for the collection, you have to have this kind of phenomenon. So, it was also for marketing.

What we see as the opt-in solution being a qualification, it's because the harvest. We don't have any case law saying that harvesting was prohibited. We said so as an interpretation. But saying that there is this opt-in solution is more clear for everybody, very simple to interpret, because sometimes interpretation, you know, for actors are very difficult. So, we had been very much supporting the project of the directive, especially because we started to have some kind of new problems within 2001.

Even with SMS, you know, that GSM is widespread in Europe. The origin of GSM is -- SMS is very much used by young people, you know, all the time sending them messages and so forth. And so, then we saw new economic business model coming up and was sending SMS unsolicited e-mail. By the way, we had to -- we brought the case to -- one big case in July last year on SMS to court and we are awaiting for the results. They are in investigation.

So, as the directive was discussed -- by the way, it had been adopted within two years, which is not very long because I always hear outside Europe that, you know, the process in Europe is very long and so forth.

Once you -- my experience, because I had been working also in Brussels -- is that once you put a new subject, a new field of legislation, it takes longer. The general directive took seven years, the whole thing, you know, preparation and premeditation.

But once you are in a field, new initiatives can come very fast, and that's the case for these two directives, which compliment the general one, which has been, I think, one year and a half and one year for implementation.

At that moment, of course, lobbies were made in member states to go back over the discussion you had here I would say, and now it comes back for the implementation. We can always repeat the discussions, okay.

So, we opened this Spam box in July. I have to say that my president took the idea to the FTC telling me, the FTC opened a box, we should do that. We did it during the summertime in July. 3,500 Spam came to us every day non-stop, even in August -- you know, August in France everybody is on the seaside. No, we were getting them.

The first days, we had been bombed, of course. We got virus of every kind. So, we have to fix the system and have a new contract because the message system

needed space, you know, and we still needed to work also inside. And the results are the following. They are in the paper. I don't know if there are some.

The Spam targets individuals 85 percent and 15 percent business. The most horrible figures are the language of the Spams. I'm sorry to say that 84.8 are in English. We didn't make a study on are they from England, from Canada or from U.S., but all those we had been looking at were for American enterprises. So, I would say about 70 percent.

Eight percent from Asian languages, Chinese, Korean and Japanese; 7 percent in French. I would say they are all French, maybe some from Canada; and 0.2 from other countries in Europe, Germany and Italy, for instance.

The content, you will see in my paper, are culturally different. For instance, you have a level of -- I mean, the American Spam were 12.3 in the health sector. It is only 0.9 in French. Financial, in English, 40 percent, 5 percent only in France. Porn messages, 42 in English and 55 in French.

(Group laughter.)

MS. GEORGES: What a joke. On this basis, they were not complaining of the content, they were complaining about the unsolicited --

(Group laughter.)

MS. GEORGES: So, what we decided was that it was time to continue to bring the cases to court because all the petit grazi (phonetic) was not enough. But we did, also, a huge campaign of petit grazi with professionals, with direct marketing associations, with consumer associations and so forth. We brought five cases, one American, in different sectors with different manner of Spamming. One French was using relay from outside Europe, of course. One French had a remote address in Los Angeles and was registered in South America, things like that, you know.

So, I completely agree with all those who say, even if Spam is international, they are originated from somewhere and the French were in France and the Americans, I guess, are originated here. So, what we see for the future that -- I mean, I won't go through the sanctions power we have. We can, in the discussion, say what they are --

MR. STEVENSON: Why don't we come back to that part of it because I think we want to just --

MS. GEORGES: Yeah, yeah. But for the corporation, I would say, the most efficient is, first, that each of us on the basis of clear law, because for good practice and so forth, make his own job to clean the

market and you will save the others outside. We will do it and, of course, we may need some cooperation. Thank you.

MR. STEVENSON: Okay, thank you. Why don't we turn now to FEDMA, the Federation of European Direct Marketers and for those of you who know Alastair Tempest, this is not him. This is Axel Tandberg who's kindly agreed to substitute for Alastair Tempest. And I think it would be helpful if we can hear from your group what the main concerns are that you've had in looking at the member state legislation and also the European Directive on electronic communications privacy as it's in the process of being implemented.

MR. TANDBERG: Well, yes. First of all, I'd like to thank the FTC for giving us the opportunity to come here. It's a great honor for us, the European Direct Marketing Association, to be here to give the European perspective.

Now, I'm going to try to speak a bit. First of all, you have to excuse me if you don't understand what I'm saying. I'm not a native English speaker, as most of us here are not. So, if we say something funny for you guys, sorry, we're speaking Brusselwaza (phonetic).

First of all, we have been working closely together with both the Commission, the Parliament and the

EPAs in Europe. Europe has had a direct data protection law legislation that Marie referred to since 1995. This has made harvesting -- we completely supported the French and harvesting is illegal. You have to have given the right to opt-out straight away when you collect the data in Europe. So, on that tone, a lot of Spam was already illegal in our sense. But the question is, of course, how do we define Spam. I won't go into that debate because you already have that one.

But to return to the new directive that just came out, we had a long discussion with the people in Europe about this. The problem we see with the new directive is how do you get the permission, because I get the question every time from members in Europe saying, can I send an e-mail asking for their permission. And I say, no, you have to have it before you send the e-mail. This isn't a way that you might say, the Commissioners tried to get a best practice. I think it might be good for business to do that because you get a closer relationship, but yet again, I'm not saying that is the best way.

The best way forward would be, as our friend said about the roaches, we need tools, we need a tool kit, we need different things, we need not just legislation.

But to go on to the issue of will opt-in solve Spam, I'm sad to say no because as we've seen, a lot of e-mails comes not from the -- comes from outside. We did a study, together with others, in I think it was 2001 where we had done sort of income unofficial studies of ourselves opening e-mail boxes and checking what comes in, and unfortunately, 60 percent comes from the U.S.

Can anybody tell me what the 40/40/40 plan is? I haven't got a clue and I still get this.

About 35 percent was from -- sorry, about 15 percent was from Asia and about -- I have to get my corrections right here -- about 22 percent was outside the European Union but within Europe, that means the associated states becoming states, other states in Europe. Three percent was from within Europe and 1 and a half percent of that was actually what we would say, untargeted, not even close to what I was. So, where are we going to?

But in five member states in Europe, they have had opt-in and they still get Spam e-mails. What we need is very good cooperation on an international level. OSD might be a solution. We're working closely together with the ICC, the International Chamber of Commerce of trying to get a solution to how we can solve the Spam issue. We also want to work very closely with Philippe, the

Commission.

We have finally been invited to take part in the next meeting of how to interpret the new directive and how to implement it in the same way in all member states because it's quite important that we don't -- with a directive in Europe, you have to interpret it according to the culture and to the legislative system because there's three different major cultures in Europe and when you come to law, you have the Code Seville (phonetic) represented by France, you have the German system which is mixed of American and -- I would say based on -- well, actually I should say -- you have the German system which is federal-based but strong interpretation by courts, you have the Anglo-Saxon way where it's basically just courts and you have the Nordic way, where I come from, where it's basically what it says in the law is right. If it says but, it must be a but in the message. It's quite literally interpreting what it says in the law.

But what we think is important to solve the issue, as I said, it's cooperation, ability for technical solutions to come up, don't stifle some technical solution with legislation that's too hard and we need to work together with consumers, internet service providers and the guys who develop the technical parts. Please don't use a sledgehammer to crack a nut. We need to do

it in the right way.

MR. STEVENSON: Have there been concerns -- I think one of the provisions in the European Directive concerns sending messages when there's a prior existing relationship, which I think Philippe referred to. Has interpreting that been one of the areas of challenge?

MR. TANDBERG: Well, we're talking in Europe about a soft opt-in. I didn't want to put that in there, but a soft opt-in we see is that they're saying you have -- you can send e-mails to an existing client to or if you have received the e-mail in the context of a sale. And the context of the sale is where the debate is going to be now and also what is a similar product and similar services. According to the Commission, similar products are, for instance, household appliances or e-mails, DVDs and books. Those are similar products.

But, yes, we do interpret it a bit differently than the Commission in the context of a sale.

MS. GEORGES: I would like to complete. This exemption is only to the point that for those who will benefit from this exemption from consent. They will still have to inform the individual at the time of collection and give the opportunity to opt-out right away by a box to check. So, it's not a complete exemption.

MR. STEVENSON: Okay, thank you. Our final

foreign panelist is actually from Massachusetts.

MS. GRANT: It is a foreign country.

MR. STEVENSON: But, actually, that's not the reason she's here. Susan Grant from National Consumers League is also the Co-Chair of the Internet Working Group and the Transatlantic Consumer Dialogue, which is a dialogue of the U.S. Government and European Commission, as well as the consumer groups from the United States and Europe, and the TACD has made Spam one of its priorities. Susan.

MS. GRANT: Thank you very much. I'm really pleased to be here today representing the Transatlantic Consumer Dialogue. Obviously, unsolicited commercial e-mails are flooding in-boxes on both sides of the Atlantic, threatening the internet as a viable means of commerce and communication. It's not just a matter of fraudulent or offensive content to us. Spam is a violation of our fundamental privacy rights and it's, obviously, not just a transatlantic problem. It's a global problem that requires a global approach.

The TACD believes that the cornerstone of such an approach should be the basic principle that commercial e-mails should not be sent without the affirmative prior consent of the recipients. If we're going to get serious about Spam, and I think our audience in the last few days

has made clear that we need to get serious, we must promote a consistent and cooperative approach that includes legislation, best practices, technology and public education. This will facilitate cross border enforcement and help us achieve our ultimate goal, which is to create an environment in the internet where Spam simply isn't tolerated anywhere in the world.

MR. STEVENSON: Thank you. Well, let's turn to a few discussion points and welcome questions from the audience. I think one of the issues I would like us to focus on for a bit is how enforcement can work in an international environment. We heard somebody earlier saying it's like a dog chasing a car, but if the dog has to chase the car across international borders and learn about the Hague Service Convention to do it and so forth, there are complications involved in the enforcement across borders.

And I wondered what our panelists thought about how that should work and how that can work even assuming that -- well, given that there are different provisions in place, how can that work? Do people have thoughts on that?

MS. GEORGES: Before saying how it can work on an international level, I would like to say if you look at the laws, you may have in national laws means for

foreigners to act. For instance, our law protects even Americans that are processed by us. So, no problem on this question. If Spam are coming from France -- not too much -- okay.

Secondly, if you have penal sanctions, our judge can act even on an international level and under international private law. The question is to execute the decision and there you need to have in the other country, some kind of, what we say, double -- the same kind of sanction.

In the case we brought to the court, we took a case in which we knew that there was the equivalent in the United States. So, you know, in those questions of unsolicited Spam, unsolicited commercially or other nature thing, you have a long list of possible criminal offense, a lot -- a lot different from fraud, from computer fraud to misrepresentation to all kinds of offenses deriving from the data protection issue.

So, for the moment, my view is that we have some hooks, even in the United States, for the moment. Of course, it would be better if we had a complete harmonized view, I think. In this case, we may have some kind of material recognition. But if you don't, it won't be.

So, how it can work? First, doing our job.

MR. STEVENSON: Okay. Peter Ferguson.

MR. FERGUSON: Thanks, Hugh. I think Marie has really singled out a number of things here similar to the European data protection, Canadian law would, for example, protect information about Europeans collected by Canadian enterprises and held in Canada. So, we already have some reciprocity and mutual recognition and there is other law where this is clearly enshrined.

I think one of the things that's going to be important here, and perhaps the United States' relationship with Europe on privacy is indicative on this. Even where there are different approaches to privacy protection, I'll single it out. There can be compatibilities and mutual recognition to some degree and protections offered around those mutual recognitions.

The other thing I don't think we want to overlook here is the very important role that the private sector is going to play in this and major international private sector organizations in organizing and building approaches to this problem, but others as well and, of course, there's all kinds of precedent for that in the marketplace at this time.

MR. STEVENSON: Would the panelists agree that there is -- well, let's take a scenario. In the NOIE report, an example of some Spam that appeared to be from

the United States that was, in fact, coming through Eastern Europe, although sometimes it's hard to tell whether it really is or whether you're led to think it is when, in fact, it's really coming from the United States. They made it look like it's from Eastern Europe and then going through the United States. I mean, there's a channel of where that's going and let's say there are people receiving it in France and in the United States. I mean, who should take action in this example and how should that happen?

MR. DALE: I think there are two levels at which we can look at this question of international cooperation and enforcement. At one level, as far as fraudulent content is concerned, and that is going to address a significant portion of the problem simply because of the high proportion of Spam that is fraudulent or almost certainly illegal somewhere in the world.

We know that, at the moment, there are a number of cooperative arrangements among agencies, including one that the FTC and a number of its corresponding agencies participate in. I think it's the International Consumer Protection and Enforcement Network. Though ultimately, I guess, that relies on sharing information about enforcement under existing national laws. But my understanding is that as far as fraudulent e-mail content

is concerned, it has been an extremely useful clearinghouse and, in some cases, has led to enforcement measures. And I think that sort of model is to be encouraged between corresponding government agencies.

But at the other level, I think that's where governments are still being a little bit cautious about agreement on policy principles here, that is Spam as Spam regardless of the content. It may be as far as the U.S. and its international policy position on Spam as opposed to Spam content is concerned, some of the issues arising from this workshop may help in a clear position not just for the U.S. but for other countries in forums like the OECD and APEC. I hope so.

I guess we have to build, to coin a phrase, a coalition of the willing as far as Spam is concerned. And I think it's easier now than it was 12 months ago. The problem is so bad, the public policy responses are starting to coalesce towards a reasonably common set of principles. But working that through bodies like the OECD and APEC, as Peter mentioned, isn't often a rapid process, but it can be done. And I think there's been a good start made by most countries.

MR. FERGUSON: I just wanted to add one further comment here. Some of this, unfortunately, has a bit of baggage attached to it and I refer to things like

governments being able to cross jurisdictional boundaries, tracing information flows, and I know the G8 has been -- the Leon Group, particularly, has been struggling with this and how do you build permissions in for that kind of thing. There are very serious diplomatic questions behind some of this. But I think the current environment really points to the need for speed in arriving at some mutually agreeable approaches.

MS. GRANT: Hugh?

MR. STEVENSON: Did you say Hugh or Hyu-Bong Chung?

MS. GRANT: I said Hugh, I'm sorry.

MR. STEVENSON: Oh, I'm sorry. We'll go down here and then to you, Susan.

MS. GRANT: Okay.

MR. CHUNG: For me, as for me personally, I think there are several things we should think about for the international cooperation. The first step we should think about is that let's promote each jurisdiction to have established rules for Spam regulation and then set up some institutional framework within the jurisdiction. That effort might be the first step we should take.

The second step we might need is to establish some kind of a network among the agencies in charge in each jurisdiction so that we can discuss or contact each

other for cooperation.

And then, the third step might be to have some harmonization proceed for the harmonization of the legal system against Spam. That's my personal opinion.

MR. STEVENSON: Thank you. Susan?

MS. GRANT: I agree with that. I think that consumers will naturally go to the authorities in their own countries first. They're more readily accessible, they speak their language. But there may be many situations where the Spammer is in another country and that agency has to have the ability to take action and also to get help from the agency in the other country. And that's why we're so supportive of the OECD guidelines that are being developed for cross border enforcement, and once those are adopted, it seems to me that there has to be some framework developed for mutual cooperation and assistance on a global basis.

MR. STEVENSON: Peter Coroneos.

MR. CORONEOS: I would agree with that. And to add, just going back to my preliminary remarks about Spam as a security issue, I mean, there is a school of thought emerging which says that if you release enough volume of Spam onto a network so as to impede the ability of that network to function, that that's tantamount to an attack on the network.

And Australia, certainly in the wake of September 11th, as I know the U.S. has done, has introduced legislation. Ours is called the Cyber Crime Act, which provides the means for agencies to actually pursue those who have instituted unauthorized interference with networks and it's just occurring to me as a vague thought that to the extent that there's commonality emerging in various nations, that that might be one basis for cross referral of investigations.

I think you need to -- my former background before I started this job was actually with the Consumer Protection and Competition Regulator in Australia, the ACCC, and I know that they've had a longstanding arrangement with the FTC and similar bodies elsewhere conducting sweeps, internet sweep days, where they determine fraud and scams and other things like that and then refer them to their sister agencies for investigation. So, I'm just raising it as a possible solution to international cooperation that you look at it. What is illegal in many jurisdictions without having to necessarily even change the laws that already exist and use that as a basis of cooperation.

MR. STEVENSON: So, I'm hearing from this discussion then that the panelists seem to -- or I guess I'm asking whether I have this consensus right. That

there seems to be a value that people see in looking to where there are rules in common, where there is some degree of a common approach as an aide to enforcement, that there is support for developing a network or networks on an enforcement level to coordinate how enforcement would happen and that there is a value to sharing the information necessary to pursue these cases.

Is that fair or do people have qualifications or comments? Philippe?

MR. GERARD: Probably -- yes, just a comment on the previous question, also. It's true that we have already some kind of legislation levels. We mentioned the Cyber Crime Convention for the big problems like hacking and that is being designed to get out with the United States. So, it's more a question of implementing this.

When you're talking about fraudulent, I think that most countries of the world have similar provisions. So, it's a question of just starting cooperation tomorrow if you want.

Now, there is another issue which is about Spam. If we go beyond, as we did, as Australia is considering going, and other countries like Korea, if you consider going beyond fraudulent Spam and you're talking about opting, there you need this kind of similar

approach because the more similar the system will be, the more similar the rules will be throughout the world, I mean, the better the enforcement will be. There's no -- you know, it's quite natural. I mean, if you don't have the same rules, you don't want to cooperate because you don't see a reason to do that.

If you have the same kind of values shared, in terms of what should be banned, how to clean up the Spam problem, then it's easier than to cooperate once you've got similar rules. I'm not -- you know, it's easy to say when you've got rules in place probably because then you kind of set the standard, but I think it's crucial in this area.

MR. STEVENSON: Mr. Tsuchiya.

MR. TSUCHIYA: I'm sorry, but I have a skeptical comment because I'm not working for a government agency or a public sector, but I am very much interested in what is the internet community. And people living in the internet community or cyberspace don't care jurisdiction. So, they are very quick. They have better -- they will try to avoid any rule or go beyond the legislation or something like that.

So, raising awareness must be first. So, coordination between law enforcement agencies takes much time. So, like-minded countries like G8 is easier, but

more international, wide area of coordination of ITU or UN takes much time. So, putting people realize that, what is Spam and Spam is not beneficial for the public. So, this must be the first choice.

MR. STEVENSON: Thank you. Yes, ma'am?

MS. GEORGES: From the enforcement point of view, I think the first time cooperation -- and we asked the Commission to organize this cooperation on an international level through a question that we had some weeks ago. I think that the first effect would be to stimulate those authorities in other countries who don't do their job, if you see what I mean.

It will be stimulation before talking about exchange of information on logs and everything. It is very easy to know where this panel originated. It is not a question of roots of IP and so forth, I can assure you. Some others during this forum said so and I completely agree. And so, the best thing in the cooperation is stimulation. We are going to have it in Europe, of course, because there is a challenge to implement this directive in a very strategical coordinated way.

We have to act at the same time with the same goal because if some of us enforce and some others don't, you see what will happen. So, we are going to have this coordination, and on an international level, it will be

very interesting to have a coordinated policy at first and this would be very effective, I think, because I'm sorry, sir, but laws are enforced mostly nationally. We are in a democracy and it's not because internet is somewhere or anywhere. We have laws and we implemented them where we are competent to do so. That's the legal system, you know. So, we still need cooperation on the international level. Thank you.

MR. STEVENSON: Peter?

MR. FERGUSON: I have just a very brief observation and following up on Marie, I agree we need international agreement on what it is the harms are that we're addressing, and that's a policy discussion. Then the rules become obvious or more obvious and appropriate.

MR. STEVENSON: Thank you. Do we have any questions from the audience?

MR. KELLY: Hi, Bennie Kelly. One thing we've been talking about in the panel over the past couple of days has been the use of some kind of symbol in the subject line, ADV or whatever the appropriate would be for the language. We do have some panelists here who's nations do implement that. I guess the question would be, given the disputes that we've had so far, what are basically the benefits of that approach? And two, do ISPs then screen those out and does that discourage

compliance by Spammers?

MR. STEVENSON: Would somebody like to address that?

MR. CORONEOS: Well, I think this is one of the weaknesses in a legislative approach in and of itself is that -- speaking as a lawyer here as well as an industry activist that tries to generate actual outcomes, the problem with any legal solution, in and of itself, is that of course the people that have got the greatest -- the ones that you're trying to target, have got the greatest motivation not to comply.

And I think, you know, that really the reason that you would legislate is to do a couple of things. Firstly, to send a clear signal to the market as to what is and what is not acceptable practice.

Secondly, you would do it because you would hope to move towards some degree of cooperation from the industry. I've been told and I've not been able to verify this, but there are some elements within industry that are not yet prepared to act, while the conduct itself is not technically illegal. So, to actually create an offense gives you a foothold to get industry attention and cooperation where, at the moment, they may be reluctant to do so because they may be concerned about their own liability in taking preemptive steps.

So, you know, it's not that it's a bad idea, but then the question is, how then do you complement that with technical solutions so that for those that aren't prepared to comply with the strict letter of the law then you've got some other means of catching the Spam.

MR. STEVENSON: Alex?

MR. TANDBERG: Axel.

MR. STEVENSON: I'm sorry.

MR. TANDBERG: That's okay, I'm used to it. The thing about labeling, I must say, will not really work because if you use the abbreviation ADV, it will work in English-speaking countries. But where I'm from, we don't say advertisement, we say reklam (phonetic). Reklam -- is that the abbreviation that will be REK recommended?

Now, I say labeling is not the answer and a Spammer -- a Spammer doesn't give a damn about the law. He will not set ADV in front of it. That would be -- the marketers would do that. So, the only ones who will follow the law will be the ones trying to be legitimate marketers and not -- you won't get to the Spammers through that, I'm sorry.

MR. STEVENSON: Motochiro Tsuchiya? Susan Grant?

MS. GRANT: I just wanted to address the issue

of public awareness. I think the public is very aware of Spam and that's why we're here today because people are demanding action. What I think will be really crucial in terms of public awareness going forward is making sure that people know what their rights are in those places where there are legal rights in this regard and where to complain, especially since it can be confusing. You don't know whether to go to your own country or to another country.

I think the econsumer.gov website that the FTC and several other countries have set up to capture complaints about internet fraud and the complaint system that we have at the National Consumers League for capturing that information, those are good models that should be promoted around the world so that complaint information can be captured in a meaningful way, not just put in the refrigerator, but gotten to agencies in realtime to take action.

MR. TSUCHIYA: I'm a political scientist, but I am believing technology motivates politics and ADV as a labeling is working. Japanese people are communicating with more Japanese people and European people with maybe Russian people is communicating with Russian people. So, their own language works. And if we can coordinate those labeling internationally so we have a list of ADV or a

Japanese label or a Chinese label, so it can be easy to opt-out via software.

MR. STEVENSON: And I think the Korean law has a provision on labeling. How is that working?

MR. CHUNG: Oh, yes. Well, let me just briefly speak about the purpose and the background of these labeling systems. The purpose of instituting this framework is to give the consumers an easy and convenient way of filtering out of the commercial advertisement at all. I mean, if somebody doesn't want any commercial e-mail, he can do it simply because most of the e-mail programs provide such kind of functions at the market. So, he can do it and some -- of course, there is a legal system saying you can go to civil suit or a court. You should think about the cost of suit or lawsuits. So, we should provide some simple way of filtering or refusing from the first step of receiving commercial advertisement.

If somebody does not want to receive any commercial e-mails, he will do it. So -- and then how we can -- the second thing I want to mention to you to enforce this framework is that it really needs some -- it is really a resource-consuming framework for the government. We implemented it -- we introduced this enforcement from July last year and last year the public

submitted the unlabeled commercial e-mails to our office and most of the complaints were composed of this complaints and we prosecuted. We levied surcharge or penalty to the e-mail centers without this labeling.

MR. STEVENSON: Thank you. Thank you very much. I think we, unfortunately, are out of time, but it just sounds like we need an internationally recognizable symbol for Spam, and we thank our panelists for their contributions and for coming so far to be with us. Thank you.

(Whereupon, at 12:15 p.m., a luncheon recess was taken.)

AFTERNOON SESSION

MR. GROMAN: Good afternoon. My name is Marc Groman. I'm an attorney with the Federal Trade Commission here in Washington, D.C. I do realize that this is the eleventh panel in a three-day workshop, that it's 1:30 p.m. on a Friday afternoon, and you all just ate lunch. That being said, I guarantee you this panel will keep you awake. Because not only do we have five esteemed attorneys up here, we have five litigators.

(Laughter).

MR. GROMAN: And the topic this afternoon is Spam litigation. Unfortunately, if you look at your agenda, you'll note we did lose a panelist. Ken Wilson, who is Defense Attorney for Etracks couldn't be here because he had a litigation emergency. But I have full confidence that the five remaining lawyers will fill up the time without a problem.

(Laughter).

MR. GROMAN: For the past three days, we have heard numerous people say that increased litigation and increased law enforcement is the Spam solution. Others, however, have noted that litigation in law enforcement has serious limitations. This panel is going to look at the practical challenges that litigation attorneys face when bringing cases against Spammers. And we're going to

look at these practical challenges with an eye towards the big picture. Is litigation and law enforcement indeed the solution? Or are we kidding ourselves and are we about to engage in the courthouse version of Whack-a-Mole, where we're going to bop a Spammer in a lawsuit over here and another one's going to pop up out of a different hole. Or worse, the same Spammer, new hole, different identity. Is that where we're going?

The individuals who are going to address these complex issues are as follows. First we have Pete Wellborn who has litigated numerous cases on behalf of Earthlink, including a $25 million judgment he obtained in 2002 on behalf of Earthlink. He also teaches internet law at Georgia Tech.

Next we have Jon Praed. Jon is a founding partner of the Internet Law Group in Virginia. He has litigated numerous case on behalf of both AOL and Verizon, including Verizon v. Ralsky and AOL v. CN Productions. Currently, Jon is litigating the five new cases announced by AOL just two weeks ago.

To my immediate right is Dietrich Biemiller. Dietrich is an attorney in Washington State who is a solo practitioner and who represents small ISPs and individuals who sue under the Washington Anti-Spam Statute, litigating the private right of action that

we've heard so much about this morning.

To my left is Paula Selis, who we have heard from this morning. Paula is with the Washington State Attorney General's Office. Indeed, she is the head of the Consumer Protection High-Tech Unit and has been intimately involved in the four cases that have been brought out of her office.

All the way on the end is Stephen Kline. Stephen is a former Assistant District Attorney and is currently with the Internet Bureau at the New York State Attorney General's Office and recently has prosecuted the MonsterHut e-mail case on behalf of that office.

We're going to go directly into questions, but I want to let you know that I promise a large amount of time at the end, because I know that members of the audience are anxious to cross examine the trial attorneys up here.

(Laughter).

MR. GROMAN: Litigation challenge number one. It's been alluded to this morning by Paula and by others, to have a lawsuit, you need a defendant. So, how easy or difficult is it to find a Spammer and how do you go about doing it? Let's start with you, Pete.

MR. WELLBORN: Finding the defendant in a Spam case is about 98 percent of the battle, but that being

said, once you find him, it's usually a slam dunk on the liability. I've been a little surprised at some of the conversation that implies there's a gray area. If you send Spam into an ISP that you know prohibits Spam, that's illegal. But finding the defendant, if you know the tricks of the trade, and the more you do it, the more you learn, it's not as hard as it would seem.

I think somebody made a very astute comment this morning that -- I think it was Dave Kramer -- one common thing that every piece of Spam or virtually every piece of Spam, except pump and dump, which is a different conversation for a different time, every piece of Spam is trying to separate you from your money, so it can have a false header, a false remove-me address, a false corporate name, but it has to have one bit of true information, maybe it's an 800 number or a fax number.

A little translation here, in Spammer-speak, suite means Mailboxes, Etc. box, but it might have a suite to send your money to, but there's got to be some true bit of information for you to get your money to them. And if you start backtracking, it's just good old-fashioned detective work. And I keep thinking at some point we're going to hit a case where we rush in to get the defendant and it's an empty house, whirring with computers, and there's no such person, but every case

we've had, we've found who we're looking for.

MR. GROMAN: So, Pete, finding the Spammer is not about high-technology issues, it's really just follow the money?

MR. WELLBORN: It's about both. What's scary, though, is that technologically, as a lot of the panels have alluded to, we're in a game of -- I think someone called it an arms race. It's a game of technological one-upmanship. And, so, if a Spammer really knows what he's doing, you can chase your tail from whichever stand that we were talking about this morning to China, to the third-party relays. So, in my experience, if it's an inexperienced Spammer or a sloppy Spammer, if he forgets to dial star-67 when he dials into the pop and you get his caller ID, fantastic. Otherwise, usually the best and quickest way to find him is to track the money.

MR. GROMAN: Okay. Jon, you're currently litigating, I believe, five new cases that AOL announced two weeks ago. I believe four or five of those cases are actually AOL v. John Doe, which means at the time the cases were filed you didn't have the identity of the defendant or the Spammer you wanted to sue. How does that work? Are you going to identify those individuals or corporations?

MR. PRAED: Well, certainly I know that AOL --

MR. GROMAN: Please talk into the microphone.

MR. PRAED: AOL has every plan to do what it takes to discover them, if they're discoverable. Three of the lawsuits name purely John Does. One of the five lawsuits does name some individual defendants but also has some John Doe affiliates that we believe were affiliated with some of the named parties. But we're engaged in discovery. We've just been granted permission to conduct John Doe discovery, which is one of the first hurdles you have to get over. And AOL's now in the middle of discovery.

MR. GROMAN: You said AOL is going to do everything it takes to find the Spammers. What does it take?

MR. PRAED: Well, it's changed over time. I wanted to echo some of the things Pete had suggested. When Spam first started, we were seeing what I call direct Spam, first generation Spam where people were simply registering a domain name, Spamming from that domain name and advertising that domain name, oftentimes adult content, oftentimes trying to sell the very products that they were using to send the Spam.

Once Spammers figured out that that was pretty easy to catch, they started then doing it through false registration of those domain names, but that was also

fairly easy to catch, so you saw a second generation develop pretty quickly in the late '90s of the affiliate model. We took that model on in the AOL v. Cyber Entertainment case, and I think that judgment resulted in what is really a fairly good model for how affiliate programs need to be run.

The current generation of Spam is really an amalgam of different types of tactics, the most sophisticated of which involves movement off-shore, using ISPs and IP addresses that make it difficult to find out who you are or funneling your money through entities that make it difficult or because of their business structure make it difficult for you to find out who the ultimate Spammer is.

MR. GROMAN: Okay. I'm going to turn to our government now, which if you get confused, is to my left. Paula, General Gregoire referred to a case out of your office that took 14 pre-filing subpoenas to find a Spammer. What challenges do you face in the Attorney General's Office trying to find your defendants?

MS. SELIS: Well, that's a very good example of why it isn't always easy to track a Spammer. There are really two ways to look at these cases. You can either go against the seller, in which case you have an easier battle, because you can always tell who the seller is,

the seller wants to sell you something and you can usually figure out who that person is.

But what we've found recently is that the seller is never the Spammer. There are two different entities, and as Jon pointed out, there are often a lot of steps in finding out who actually did press the button to send the Spam. And in the case that you were talking about against a guy named Samuel Meltzer out of Minneapolis, I'll tell the war story here, because I think it demonstrates the problems.

We had complaints about a Spam that people were receiving that said something like board meeting three-ish, that was the subject matter line. And you opened it up and it was an ad for a debt adjustment company. And the debt-adjustment company site had a form that you could fill out if you were interested in getting debt-adjustment services, and people would fill out the form.

And obviously this is a violation because there was a misleading subject line. There was also a false header. So, we figured, well, we'll just contact the debt-adjustment company and find out who the Spammer is, you know, how do they get their leads. Well, we contacted them and they said, well, we don't know, we contract with a company in New York who gives us the leads.

So, we contacted them with a pre-suit subpoena. We'd already sent one to the company in Florida. And the company in New York said, well, we contract with another company in Chicago. We sent a CID to the company in Chicago, and so on and so on and so on. We found out that really ultimately we couldn't trace the Spammer that way. What we wound up doing was finding out where the Spammer was hooked up at the time the ad was run, what the IP address was. We found out that it belonged to Microsoft, we CIDed Microsoft, who in fact had leased out that line to another company. We had to CID that ISP; found out who the line was leased to; of course it wasn't leased to the Spammer; it was leased to somebody who used a fake identify.

Ultimately, the way we found out was that the credit card that was used to pay the ISP was under one person's name. We found out who put the money in the account, who paid the bills on that account, and that way we traced it to the Meltzers. Now, you know, that's a lot of steps. That's 14 pre-suit subpoenas, and that gives you an idea of how difficult it is. And when you look at the resources --

MR. GROMAN: Let me ask you a question. What ultimately happened? So, that's an enormous amount of work for one Spam case. What ultimately happened in that

case?

MS. SELIS: Well, we sued Mr. Meltzer and we got a judgment against him.

MR. GROMAN: For how much?

MS. SELIS: $10,000, which wasn't a lot, but I think it was enough to keep him from Spamming again, in our state, at any rate. And we had spent a lot more than that.

MR. GROMAN: Right.

MS. SELIS: So, you know, a sort of happy ending, but, you know, not exactly an economical one.

MR. GROMAN: Okay, let's hear from Stephen. Same issue, tracking down the Spammer.

MR. KLINE: Yeah, exact same problems that Paula had. We'd been receiving several thousand complaints a year about Spam, and when we first started focusing on this issue, we started doing it the same way, so we'd get the complaints in and we'd start going backwards. And it was beyond frustrating. It was too time-consuming, and in the end, you know, a lot of the Spammers weren't within the jurisdiction or in the end maybe not even worth going after any further.

MR. GROMAN: So, you have examples of cases where you open up the matter, start the investigation and then have to close it?

MR. KLINE: Yeah. And so we figured that there must be a more efficient way to find the evidence. And, so, I started reaching out to the ISPs, figuring that they were the ones who knew the most about where the Spam was coming from and all of that. And it's worked pretty well. The ISPs that I've met with, I usually meet with their attorney and their abuse team. And the abuse teams have been giddy, that somebody is actually wanting to prosecute.

MR. GROMAN: Well, on that note, have you -- talking about the challenges that you're facing with ISPs, have you had a situation where you've served a subpoena on an ISP and then had one of two concerns, you either found that the evidence you needed or data you needed was no longer available, or you had the concern that the ISP might actually notify the subject of your subpoena?

MR. KLINE: We always run into the situation where the data is no longer available. But if it's a Spammer that they're continuing to have problems with, you know, they're going to have the data available. They may not have all the data about the Spamming history, but they're going to have some of it. So, that's how we actually picked up the MonsterHut case. It wasn't an ISP that we had talked to, but it was a referral from another

ISP and the ISP came to us and said we are getting killed with these bozos up in Niagara Falls, and it was great, they had all the evidence, they had been collecting it for their own lawsuit, and it worked well.

There have been other times where we've reached out and for one reason or another it hasn't worked out. So, we're still trying to figure out the best way to handle it, but I think going to the people with the evidence, rather than -- and saying who's in New York, who's Spamming from New York, has been a lot more successful than trying to get the Spam from consumers and then going backwards.

MR. GROMAN: Okay, thank you.

MS. SELIS: Can I address that second question, because I think it's a valid one?

MR. GROMAN: Please, please.

MS. SELIS: What happens when you subpoena information from an ISP and that ISP has a privacy policy that says that we must tell our customers if there's been any inquiry about them or any subpoena. Actually, the states have a mechanism where you can go into court and ask the court to order the ISP to keep the fact of that subpoena confidential, and we have done that consistently and it has worked quite well.

MR. GROMAN: Dietrich, in your cases, your

clients are not Earthlinks or Verizons but smaller individuals. My understanding is that when they come to you with a case they already know who the Spammer is. Is that correct?

MR. BIEMILLER: Usually. And ours is not as much a problem of tracking them down, but choosing who to sue to begin with. We have to go for the low-hanging fruit because we just don't have the resources of a large firm or the government. So, if we have a clear line of sight and a large number of Spam, we will usually go for those. And generally the guys have done a lot of research and tracked them down already. And I follow up and make sure that it's the right person before we go and off we go.

MR. GROMAN: Okay, well, that's a good segue into the next topic I want to discuss, which is who in fact do you sue. Paula, you stated that the Spammer is never the same person as, what, the marketer?

MS. SELIS: The merchant.

MR. GROMAN: The merchant. So, I'd actually like each person to address that. Who do you sue? You could have a situation where you have a Spammer, someone selling a product, an advertising company, an e-mail marketing company and an affiliate program. There are contracts between all these entities, or maybe not. So,

who is it? Who is it that you choose to sue? I guess -- I'm going to start with Jon on that, because you have the five new cases, and I've looked at them. It seems to me that your approach is sue everybody.

(Laughter).

MR. GROMAN: But how does that work?

MR. PRAED: I don't know that I want to address in particular decisions on any particular case, but I think generally my approach is to sue as big a fish as you can find. I spend probably a majority of my time actually trying to identify characteristics, I call them fingerprints, that constitute a big fish and then target a lawsuit against that individual or group of individuals.

And it's really -- you're looking in the end for someone who is sending unsolicited commercial mail using some sort of fraud, and it is a target-rich environment. You talked earlier about Whack-a-Mole. That is the risk that you run, that you are simply playing Whack-a-Mole. I think both on the filter side and on the litigation, you have to systematize what you're doing so that you're not playing Whack-a-Mole.

Litigation is critical, though, because I think it is your best opportunity to make the mole pull out his driver's license and actually show you who he is, so that

you can thereafter -- he's been bagged and tagged, in a sense.

MR. GROMAN: On the issue of who do you sue, if you've got a situation with multiple parties involved, you have a merchant who hires a marketing company, who maybe goes through an affiliate, and then we end up with an individual who sends out the Spam and pushes the button. And the Spammer changes -- or someone along that chain changes the subject line or makes it a deceptive subject line, and you want the big fish who may be on the end. Why is that party liable? Why can they be sued?

MR. PRAED: Well, you can make all sorts of arguments to why they should be and why they shouldn't be. In the end, though, Spam conspiracy and assistance, liability for assisting Spammers is not that much different from liability for any other type of illegal conduct. Conspiracy is an old established theory of law. We're not inventing very much law here, really. We're simply trying to take -- in fact, I think one of the best provisions to go after Spammers trespassed the channels. It predates the Constitution. It's not rocket science. The trick is simply getting everyone to agree and understand that these fairly basic concepts of legal principles can be applied in a very new arena in some factually unique circumstances, where identity and really

identifying who is the big mole is the real issue.

MR. GROMAN: Pete, who do you sue and why?

MR. WELLBORN: I'm going to answer that in two parts. I think of Spammers much like Dante's levels of hell.

(Laughter).

MR. WELLBORN: There are ascending levels of egregiousness. At the bottom we have -- we'll call them vanilla Spammers. Those are the ones that send unsolicited commercial e-mail through ISPs that they know forbid that e-mail. It's not spoofed; it's not fraudulent; it's not selling herbal products; it's not selling illegal descrambler boxes. That's your lowest level.

Compound that by spoofing and by some of the fraudulent tactics that we've heard about for the last two days. Compound that even more by Spammers who are selling these fraudulent or illegal products. That's the next level. Then there's a top level of egregiousness that the Spammers that are doing all those things and using accounts that are purchased with stolen credit cards or by identity theft to send these e-mails.

So, you have those three levels. And as Jon said, what we've done so far is we've gone after the top level, the old saying that the squeaky hinge gets the

grease, well, that's the one that we've gone after. After sitting through these panels for the past couple of days, I'm convinced that we need to start going after the lowest level to send a message, because it seems as though there's a fundamental misunderstanding that if you're not spoofing and you're not selling a fraudulent product your unsolicited commercial e-mail is somehow legal or at least a gray area, even if you're sending it through the ISPs of the world who forbid Spam. And that's wrong.

If you knowingly send your Spam into an ISP that forbids Spam you're committing a criminal act. You know, there was a lot of discussion this morning about do we -- we need a criminal statute, we need a Federal statute. We've already got them. We've got a criminal statute, it's called the Computer Fraud & Abuse Act. We've got other criminal statutes. It's the state prohibitions against common trespass, the same thing that keeps someone from walking into your house and getting on your computer, keeps them from sending unwelcome Spam into the ISPs. So, let's sue some of these lower level Spammers and send a message that we're not going to only go after you if you're committing credit card fraud --

MR. GROMAN: Pete, when you say let's sue, who do you mean? Who's let's?

MR. WELLBORN: Let's -- the ISPs that can afford to bear the mantle of the battle, for starters. The Earthlinks who are doing it right now; the AOLs and the Microsofts. For now, with as much cooperation from the government and from law enforcement as we can get, I think these need to be the mantle bearers.

MR. GROMAN: Okay, Dietrich, back to you on the same topic. Your client comes into your office with the Spam e-mails, says I've identified who it likely is, I'll use your term, you want to go after, what was it, the low-hanging fruit?

MR. BIEMILLER: Low-hanging fruit.

MR. GROMAN: Who is that?

MR. BIEMILLER: It's somebody who -- first of all, we can't afford to do what Paula does with spending a huge amount of money and getting a minimal return, so we have to -- one of the things unfortunately we have to determine is whether they have money or not to pay a judgment or to pay a settlement. And most of my clients are pretty anti-Spam-active folk, and they go after the highest circle of hell there, and so usually those -- if we can find somebody that combines those qualities and we can identify them, that's a likely target.

MR. GROMAN: Stephen, when you're at the end of your investigation, you're making a determination of

whose name, what corporation, what individual's name goes on your complaint, what factors are you considering and does jurisdiction become an issue there?

MR. KLINE: Yeah, jurisdiction is always an issue for us, but when we are trying to figure out who to sue and why, you know, we -- it's a little -- the Spam cases are a little bit different for us than the rest of our cases, because normally what we're looking to do is get restitution back to consumers. Here restitution is such a tough thing to calculate per Spammer. And then any sort of damages are also tough to calculate.

You know, we do consider whether they have money, but what our overall purpose is to do is impact litigation. And if we wind up with an empty judgment but the precedent that we set will steer the industry in the right direction, I think that is the major concern that we have.

MR. GROMAN: You mentioned the issue of jurisdiction and you said that's always a factor. Can you explain why that's always a factor?

MR. KLINE: Well, because we represent the state. We generally prosecute corporations or people doing business in New York. We have in the past sued people from out-of-state for injuries in New York, but in cases like the Spam cases where we are going to have so

many other issues to deal with, and there are Spammers in New York, you know, we try to cut our litigation risk and focus on the bad actors in New York right now.

MR. GROMAN: So, if you have an investigation that's open and you ultimately discover somewhere down the road that the Spammer's actually in Texas, what do you do with that case?

MR. KLINE: Most likely we'd refer to the Texas AG or the FTC.

MR. GROMAN: Have you had luck referring those kinds of cases to other states?

MR. KLINE: We haven't had to do that yet. We've -- you know, we've gone to the ISPs and said who's in New York, tell us where they are, tell us what's happening, and we've kind of gotten to pick and choose our cases.

MR. GROMAN: Paula, same question. Is jurisdiction a challenge for you or is it really not?

MS. SELIS: Well, let me just kind of follow up on what Stephen was saying. When you start out in a Spam case, at least when we start out, we don't know where our defendant is going to be necessarily, true with the Meltzer case. And while in some cases you can pick and choose where your defendants are located, it's harder in a Spam case, you can't, at least not very easily. But in

terms of jurisdiction, we haven't run into any issues thus far, though Dietrich has run into jurisdictional issues.

We take the position that if you are sending e-mail to the State of Washington and the person to whom you are sending that e-mail has identified him or herself as a Washington resident, then Washington courts can, under long-arm jurisdiction, hear cases involving the defendants. So, so far, so good. I think Dietrich can talk about his case, because his defendant did, in fact, question Washington's jurisdiction, and he got a very favorable ruling.

MR. BIEMILLER: They all do. I spend about 80 percent of my time litigating jurisdiction, long-arm jurisdiction, so . . .

MR. GROMAN: Okay, and just for a background for those of us who are not attorneys in the room, the question really is if the proposed plaintiff is in the State of Washington, and that's where that person may have had their injury, but the Spammer is elsewhere, can Dietrich's client bring the lawsuit in the State of Washington, even though the Spammer may be on the other side of the country and then be forced to litigate the issue there. So, speak about your experiences with that issue.

MR. BIEMILLER: Well, that's generally the main question, and they tend to make the same arguments over and over. I mean, why should we have to go to Washington to defend this case, but, you know, the tort occurred in Washington and we exert the long-arm jurisdiction by the statute that we have. It can't exceed the Federal Constitutional issue there about purposeful availment and those kind of issues, but we've been very successful both in superior state court and federal court defending that question.

MR. GROMAN: So, you're finding that in your cases the issue of jurisdiction really isn't a challenge or a problem.

MR. BIEMILLER: Well, it was a problem for a long time, and I guess Paula can also speak to this, we just recently passed a law specifically addressing jurisdiction because it has been such a problem, for us at least.

MR. GROMAN: Okay, turning to the attorneys who represent the big ISPs, I know that AOL's cases have all been filed in Virginia. I think Earthlink's cases have all been filed in Georgia, regardless of where your potential defendants are located. So, let's look to you, Jon, first, and you litigated the Ralsky case. From your perspective, is the jurisdiction just settled, where

done, and it's not a challenge anymore?

MR. PRAED: I think it was settled before it was even started, but that doesn't keep a defendant from bringing a motion to dismiss, and I think you have to bring a Spam case, wherever you want to bring it, in anticipation of a motion. But I think that it is pretty clearly decided today in the Spam arena. I think the Verizon Online v. Ralsky case was an excellent decision that addressed -- you have a question of forum non conveniens. Can a Spammer be put to the inconvenience of being sued in the state where he actually Spammed, which is a separate question.

The real question is did he purposefully avail himself of the protection of the state into which his Spam landed. And a lot of Spammers defend by saying essentially I didn't have a clue. I fired a gun, and the bullet left the gun, and I had no clue as to where that bullet was directed, other than the e-mail address. And I think the court, in the Verizon case, pretty clearly decided that apathy, as to jurisdiction, is not a defense to a personal jurisdiction argument.

MR. GROMAN: Okay, so grandma in Oklahoma who sends out 10,000 e-mails and 800 of them actually end up going through an AOL server in Virginia, she's going to be hauled here?

MR. PRAED: Well, I have been surprised. I have yet to identify a fraudulent Spammer that actually was a grandma.

(Laughter).

MR. PRAED: If I got one of them, she's probably going to be driving a Porsche or a Ferrari, and she'll know exactly what she was doing or she won't care. I hear the point. Someone might make an argument that the mere incidental transmission of a small volume doesn't necessarily give rise to personal jurisdiction. An interesting argument, but not one that really has more than a theoretical application in most of these cases.

And one correction. AOL has actually filed suit, I think throughout the country. Certainly Virginia has been a common state for suits, but AOL has, in fact, filed I think in California, New York, many other states, in part to try to establish this fairly basic principle across the country.

MR. GROMAN: Okay, I want to turn to another issue that our attorneys face, which is causes of action. When you want to bring a lawsuit, there needs to be a law that's been broken. So, what are the causes of action that you are using or advising your clients to use in your complaints? Let's start with you, Pete.

MR. WELLBORN: Okay. And one interesting note

on the jurisdiction issue, we all owe a debt of thanks to Shirley Jones, the mother from the Partridge Family, whose landmark lawsuit, jurisdiction lawsuit against a writer and editor for The National Enquirer, gave us the most widely cited jurisdiction case when you're claiming the effects test that you can sue here because this is where we got hurt. That's a little hinting aside.

(Laughter).

MR. WELLBORN: Causes of action. I have a laundry list of about 12 or 13 different causes of action, any one of which will carry the day in a typical Spamming and spoofing case. The two most common that we see, as I mentioned earlier, the Computer Fraud & Abuse Act, Federal -- a computer-specific Federal statute that provides for criminal liability in a civil action, as well, if there's been intentional access of a protected computer system that's unauthorized and that causes damage, which that's the very definition of unwelcome Spam coming into an ISP system.

Another cause of action that we see a lot and use a lot is common law trespass. It's like I said, the same law that keeps one of you from breaking into my house, coming in and sitting down at my computer and using it, that same general law in each state also prohibits a Spammer from taking unfair advantage of the

ISP's computer system and converting the ISP's computer system to the Spammer's benefit.

MR. GROMAN: Dietrich, in the private right of action cases that you file, is the cause of action strictly under the Washington Spam statute?

MR. BIEMILLER: Typically. I mean, we do cite trespass through chattel, as well, because under their consumer protection act some of the judges have found that they need to have some actual damages in order to enact the treble damages provision of that. But typically we just have this nifty statute that Paula had something to do with, and we use that.

MR. GROMAN: Stephen, for your cases for the New York State Attorney General, New York, unlike Washington State, does not have a Spam statute. So, what is the cause of action that you used in your Monster Hut case or other potential cases?

MR. KLINE: New York doesn't have a Spam statute, per se, but I consider all of our laws anti-Spam statutes, because the same sort of fraud that's committed on-line has been committed off-line, as well. So, we've been using our deceptive practices statute, which is similar to the FTC act, but we also have a statute, Executive Law 6312 that allows us to prosecute civilly any business who is repeatedly committing fraud or any

sort of illegality, which opens the door to all the laws in New York, even common laws. So, we can -- if someone's violating the criminal forgery statute, an administrative statute, common law, all of those fall under 6312 for us. So, I feel right now that I've got all the tools I need to prosecute a Spammer. If they want to give us another one via a Spam statute, which I think they're going to, fine with me.

MR. GROMAN: What is the relief that you are seeking in your cases? You mentioned that restitution is not something you're seeking, so what would it be?

MR. KLINE: In the MonsterHut case we were seeking penalties. Under our consumer protection statute, we're allowed to seek up to $500 per violation. And the -- I think the injunctive relief is actually going to be more important than any sort of money judgment. A lot of the -- the two principals in MonsterHut, one fled to Canada; the other one ran down to Florida and is not working. They don't have any assets. So, the money judgments that we're going to get, whether it's penalties or restitution I think are going to be somewhat meaningless. So, I think any sort of injunctive relief is probably the most important thing that we'll get.

MR. GROMAN: Paula, turning to your cases and a

comment made by Stephen in that -- I know I'm paraphrasing, the money judgment is essentially meaningless or worthless.

MR. KLINE: In some cases.

MR. GROMAN: In some cases. What is the relief that you're looking for and what is your view on the money judgments?

MS. SELIS: Well, this brings up a whole question, how do you measure the injury? I mean there are a lot of injuries with the receipt of Spam, some of which are measurable and some of which are not. So, an ISP who can say his system went down for two days and he lost X amount of money has an easier time showing an amount certain.

But a consumer who gets Spammed, you know, how is he or she going to show that there is money actually lost? So, our statute has a $500 per Spam penalty associated with it for consumers and $1,000 per Spam penalty associated with it for ISPs. Or, in the alternative, if actual damages are more, then you can ask the court to give you actual damages.

Your question, though, which I haven't really answered, is how important are damages. I talked this morning about deterrent effect, and I think that's -- I have to come back to that. If you can hit a Spammer in

his or her pocketbook, then you've done a successful job. Now, some of them are real mom-and-pop operations, they're not making a lot of money, and so if you can hit them with a $10,000 judgment, that to them is a deterrent and that will make them stop.

If, on the other hand, you come up against what we'd call a Spam house, a really big operation, and I don't think we have yet to take one of those down, although I think we would like to, I would look to getting a significant amount of damages. So, I think damages are important, as long as they act as a deterrent effect.

MR. GROMAN: Okay, following up on the same path of the issue of the judgment, turning to my right, there's certainly a big difference between filing a case and getting a judgment, possibly by default and actually collecting on that judgment, meaning -- and if you're not collecting, are you really hurting someone in their pocketbook. Starting with, Dietrich, have you had the case where you've got judgments that are just not going to be collected?

MR. BIEMILLER: We've got one right now that is a Spammer down in Florida that we got a $270,000 judgment on that we're never probably going to see. The ones that we have collected money are usually ones that have

settled. They see the writing on the wall typically and will talk to us about, you know, getting out of it.

MR. GROMAN: Pete, you had -- the ISP cases tend to make really fantastic headlines that read something like $25 million judgment against Smith on behalf of Earthlink. Will you ever see that $25 million? I mean, has that been collected and what will happen with that?

MR. WELLBORN: We're currently looking for that off-shore as we speak. Will we get the whole $25 million? Who knows. Will that send a message to every other Spammer in the country, that if you Spam you'll get the financial death penalty? Yeah, that's going to send that message. And what's more, talking about the remedies, it's just as important as the money, turning back to the idea of injunctive relief, one thing that we've done for the past three or four years for, you know, for Earthlink in every case they resolve; for some of the smaller ISPs as well that I represent, when we get relief in these cases, we don't ask the court protect Earthlink from -- Earthlink and Earthlink only from the Spammer's future bad acts or if it's for Friendly E-mail protect Friendly E-mail, no more bad acts against Friendly E-mail.

Instead, we get an order from the court that

directs the Spammer never to Spam, spoof or commit any other of a various list of prohibited conduct against anyone in the world. And, in fact, the order makes all ISPs and internet users worldwide express third-party beneficiaries who can sue under that -- for a violation of that order as if it were a contract to which they were a party.

MR. GROMAN: Pete, do you think that the Spammers you see are actually complying with that injunctive relief?

MR. WELLBORN: I do, because among other aspects of the relief, this is already the law, but we stress it in all caps and bold face that violation of this order will not only be a future Spamming violation but will result in civil and criminal sanctions against these Spammers. So, if you're talking about a small amount of money or even a big judgment if they're poor, maybe that doesn't get their attention, but if they understand, and I've had judges look the defendants in the face and tell them, if you violate this, you will go to jail. And that gets people's attention.

MR. GROMAN: Do you -- I understand that you say you believe they're following, but do you do what I would call compliance monitoring? Do you have any actual anecdotal or otherwise evidence that the Spammers aren't

just starting over under a different name in a different state or location?

MR. WELLBORN: We do. There is one Spammer who has -- he backslid, unfortunately, he Spammed me personally.

(Laughter).

MR. WELLBORN: And this was a guy who got drunk and told the -- got drunk, left a voicemail on my client's voicemail saying that he was in cahoots with me to Spam the client and have the client pay me legal fees and that I would split my fees with the Spammer. And of course when I played that tape for the federal chief judge in Atlanta, Orinda Evans, and she just about had a fit. She was not happy with this particular defendant.

But he Spammed me about six months ago, three months ago, and I'm finishing up the -- my personal suit to enforce the order of permanent injunction that we got against him on behalf of a couple of smaller ISPs three years ago. So, some backslide. Others that I've checked on periodically, just knowing they were going to backslide, have not.

So, yes, this global relief, it's really important because it protects -- it keeps the Spammer from moving on to smaller ISPs or smaller entities that are less able to defend themselves than the Earthlinks

and the AOLs and the Microsofts of the world, and this is something we all should use. I mean, I'll be happy, if anyone in this room is a Spam plaintiff and you want to e-mail me, I will send you the legal brief that explains why that relief is appropriate and explains to the court that the legal basis for awarding that universal relief, even if the plaintiff is only a single company. I'll give you my e-mail afterwards, and I will send that to you the day you e-mail me.

MR. GROMAN: Okay, Jon, we'll give you the last word on this idea. First of all, judgments, are the big headline judgments that aren't collected, is that still a deterrent? And then second of all, is this injunctive relief doing anything?

MR. PRAED: Yes, to both. Press is obviously an important part of what we're all doing, trying to get the message out there. Judgments are the first step. The first step is really before that. The first step is making Spammers realize that every step of the way there's going to be an increased cost to the business. They operate typically on fairly thin margins. Those that are making a great deal of money are working very hard to try to do everything they can to hide. And if you can get a judgment against them, even if it's not collectible today, that's not to say it's not going to be

collectible tomorrow, and it's very difficult for Spammers in my experience to discharge Spam judgments in bankruptcy. That's a message that I think too few Spammers realize.

But at the end of most of the cases that I have been involved in, the Spammer has been quite upset by the path that they have put themselves on. They understand that they've -- I wouldn't say ruined their lives, but they have made some tremendous mistakes along the way. Even if they can't write a large check at the end, they realize they're never going to be in a position to write themselves a large check for a very long time.

And that has an effect on them and it obviously has an effect. In fact, if this is a game of Whack-a-Mole, your focus is largely on general deterrents and not specific deterrents. And I think anyone who's thinking of getting into the Spam game needs to think twice when they see that many of the major players who are involved in the internet space are committing significant resources less towards recouping their costs of litigation but rather towards generally reducing their cost of hardware investment and of increasing the cost on the Spammer.

MR. GROMAN: Okay, thank you. Let's turn back to the idea of a private right of action, which had a lot

of attention this morning on the legislation panel. There are those who believe that giving individuals who receive Spam a private right of action to sue will have an enormous deterrent effect.

So, Dietrich, I'll turn to you on this. First of all, who are your clients and what are these lawsuits about?

MR. BIEMILLER: Most of them are tech-savvy ISP or tech people. I do have a small ISP. I've got a landscape design engineering company that got relay-raped. So, it's mostly -- I mean, I don't do any advertising, it's mostly word of mouth and people hearing about it through either media or friends.

MR. GROMAN: Are you litigating these Spam cases full-time?

MR. BIEMILLER: Yes. Well, yeah, among my other practice, but I'd say the majority of my stuff right now is Spam cases.

MR. GROMAN: And how do these private right of actions get resolved? Are these judgments, default judgments, settlements?

MR. BIEMILLER: All across the gamut. We do settle; we do default judgments. I haven't actually had one go to court yet because we just started doing these like last July and the court dates aren't, you know, that

speedy as we all know, but we're progressing through discovery on most of these right now.

MR. GROMAN: I'm going to ask you a question that I know that a lot of other attorneys have been wondering. Does this make financial sense for you? Are you making --

MR. BIEMILLER: I'm certainly not making money like I would like to, as if I had a large-firm job. The big payout at the end is quite the carrot though, if we do get a large judgment against somebody who actually has money and who actually pays it, which is three pretty attenuated things. But the settlements are kind of providing a war chest to go file more cases and proceed with the ones that are in the middle.

MR. GROMAN: Who's covering the cost of these private right of action cases?

MR. BIEMILLER: Right now, the co-counsel I have, Mr. D. Michael Tompkins, who I rent space from, is fronting most of these, but there really aren't that many costs. I mean, we try to do it on --

MR. GROMAN: So, it's not the client, then?

MR. BIEMILLER: No, no. We haven't had that many costs. Mostly it's just filing fees and that sort of thing. We haven't done a lot of traveling and that sort of thing.

MR. GROMAN: What is the goal of private right of action cases?

MR. BIEMILLER: Well, the goal of the client is to get the Spam to stop to them individually. And part of every settlement that we've had we do get the injunctive provisions, kind of like Pete was talking about, and it works for them. I mean, we obviously don't have the power to extend that -- well, I guess maybe we do. I'd like to get that brief from you, Pete.

(Laughter).

MR. BIEMILLER: I might be trying to get that incorporated, as well. But so far it's done a good job for them individually, but we do have the Whack-a-Mole situation, but if we want to go back to the analogy earlier today, the viral thing, I mean, if we whack one mole, if we just stop whacking them we're going to be overrun with moles. So, you just have to keep whacking until the problem changes.

MR. GROMAN: Why does an individual who wants to file a right of action or a small company, under the statute, need a lawyer? Shouldn't they be able to --

MR. BIEMILLER: Yes, we do have small claims in district court that they can go to. The ones that come to me, though, are typically large volumes. Like some of my clients have 300 or 400 Spams that they want to deal

with from real prolific Spammers. And those -- they tend to get in over their heads when they start getting removed to federal court and that kind of thing.

But one of my other cases is a guy who won in small claims court and they've appealed that all the way up to the court of appeals at this point, to keep the precedent from getting set. I guess the Spammers appealed it.

MR. GROMAN: Okay, I'd like to raise the issue of abuse litigation. And since you are the member of the plaintiff's bar on our panel, I'm going to toss it at you.

MR. BIEMILLER: Okay.

MR. GROMAN: There are those who would articulate a view that Spam statutes are going to be abused by the plaintiff's bar and that it might as well just be a personal injury case, it really doesn't matter. They're going to find a statute and they're going to abuse it as a money-making scheme. And is that a legitimate concern and does it matter?

MR. BIEMILLER: Well, I guess we've heard all about Utah this morning. We don't have that problem here. I guess like any kind of litigation it can be abused, so it's really going to be an individual case type thing. I don't feel like I'm abusing it personally.

It's just like a personal injury thing; you have to have a car wreck to bring a suit on that. With us, it just seems overwhelming because we have a bazillion million car wrecks to deal with. So, if that means we're suing to enforce a lawful statute to try to stem the tide of this stuff, I can't see that as abusive.

Further, it's kind of ironic that those who talk the most about we're trying to make money off this are the Spammers themselves who by their very definition, that's what they're doing when they're Spamming, is just trying to make as much money as they can, so --

MR. GROMAN: I want to open up that same question to Jon and Pete and just see if you have anything to say about this concern that Spam statutes and Spam litigation might actually have a chilling effect on legitimate companies who are fearful of litigation. You don't have to take it, but --

MR. PRAED: I think as Dietrich suggested, abuse is not unique to Spam litigation, and the concept of abuse and the mechanisms to prevent it have been around for a long time. Rule 11 is as effective in Spam litigation as it is anywhere else. And I think that those deterrent powers are perfectly adequate to keep people from using Spam litigation abusively.

I quite frankly think, though, if you're

talking bottom line justice that I have seen far more abuse on the defense bar in Spam cases where you have a defendant who is engaging in fraudulent Spam. There have been -- I don't want to talk about particular cases, but it is not unusual for Spammers to literally throw their computers away in order to keep them from being discovered. It's not unusual for -- I think one could argue that many of the answers that are filed in response to complaints are dancing on the line of Rule 11.

Those are abusive tactics, as well, and are as worthy of concern in an age when you can debate what "is" means. I think it is a real risk to fall into the trap that Spammers think that litigation over Spam is a continuation of the game that is Spam. And I think they're learning -- you know, Virginia has just -- or has just enhanced its criminal statutes. I think the day has come when Spammers are going to realize this is not a game. And likewise, people who engage in abusive conduct on the plaintiff's side, there are adequate measures in place to prevent that.

MR. GROMAN: Thank you. I'm going to turn back to my colleagues in the state government. Eileen asked a question this morning on the legislation panel that I thought was from my panel, but she's my boss, she can do that. And it was to Paula, so I'm going to turn the

exact same question to Stephen.

Twenty-nine states have Spam statutes, and I believe we've only see action out of three states. Why?

MR. KLINE: Well, I can tell General Spitzer will kill me if I start guessing as to why other states are not acting. I can tell you why -- it's tough. I mean, you're looking at our Spam litigation team. It's me and my civilian investigator. And it's not even full-time. I've got, you know, ten other cases that I handle as well.

MR. GROMAN: And that's for the State of New York which is a comparatively big state.

MR. KLINE: That's for the State of New York, yeah. And so there are -- I think one thing that you see in both the criminal side in which I've had experience and in this side is that a lot of the states attorneys just don't have the training in high-tech cases. It's expensive. It's -- once people get training in that area, it's -- there are certainly a lot of lucrative offers that come along. And, so, I think it's, one, tough to find people who can do it; two, I think it's tough to find the money to do it. And I think in some situations it may be tough to find the higher-ups that understand what's going on or understand the seriousness of it.

MR. GROMAN: Paula, how many --

UNIDENTIFIED SPEAKER: Can you elaborate on those lucrative offers?

(Laughter).

UNIDENTIFIED SPEAKER: A little more on those, please.

(Laughter).

MR. GROMAN: Paula, how many attorneys with the Washington State AG's Office are working on Spam issues?

MS. SELIS: You're looking at the one. I am she. I agree with Stephen, everything that he said is true. And just to highlight that, Spam is, I think everybody in this room recognizes, it's a problem, and it's a huge economic problem. But when you have consumers who are calling you about the fact that they have lost $10,000 to a telemarketer and you've got to decide whether you're going to help that consumer or whether you're going to file a Spam suit where nobody's really lost any money, although the entire internet community has lost a significant amount, oftentimes you're going to take the case involving the telemarketer. And those are very real pressures, priorities that state AGs face every day. So, you know, I don't want to malign our brethren, sistren in other states, but there are good reasons for not taking Spam cases.

MR. GROMAN: I was going to follow up on that, but I'm actually going to turn that same question to the counsel for the big ISPs and say that there are those who would say that your -- the companies represented actually brought relatively few Spam cases. I think Earthlink's about a dozen. I think in total, from the press release I read about AOL, it's 25 total. And between May of 2001 and April of 2003, they brought no cases. So, why do you think that would be?

MR. PRAED: Well, I don't know that those numbers are necessarily correct, and I don't want to debate the numbers with you necessarily. I will say bringing a lawsuit, first of all, is a tremendous commitment of resources. And there have been, I think, a lot of lawsuits brought, but the bringing of a lawsuit is really the tip of the iceberg. I think you're seeing the state attorneys general bring relatively few cases because it is so resource-intensive. It's resource-intensive for the ISPs, as well, regardless of size. And, again, it's a game of Whack-a-Mole. I think there are tremendous, tremendous volume of resources being devoted, first of all, to maintaining the networks. I am amazed at the job that large ISPs and small ISPs are capable of doing.

I would challenge -- I think it's remarkable in

a sense to step back and identify any other business enterprise that is capable of withstanding essentially 40 to 70 percent free ridership problem. The Metro system here in town would collapse if 40 to 70 percent of us were jumping the turnstiles. There is no other business today that could support that level of free ridership, but it is not free in the end for the ISPs.

And what they are doing both in terms of managing the daily volume that they have and systematizing the investigation that allows them to put in place a process that culminates in a lawsuit. It is one thing to issue 14 subpoenas. Issuing subpoenas is really the last step in the process of sending letters, making phone calls, doing some very thorough investigations that provide you a great deal of information and that have real repercussions.

I'm as proud of the fact that we oftentimes chase Spammers across the network space as I am over the fact that we may sue them and identify them. Don't misunderstand. We put costs on Spammers the day we start thinking about them, not the day we start suing them. And that's the trick, is to try to find ways -- I want them in this room. We're all in a sense wasting our time talking about the problem. We need to go sit at computers and do the very hard work that the major ISPs

and the government officials and the solo practitioners are doing.

MR. GROMAN: I have a question to follow up on you, and I'd like a quick answer on this one. Do you subscribe to the point of view that there really are 150 big guys out there doing most of the Spamming?

MR. PRAED: I don't know that that number's right, but I think you'd be shocked by how many few very big fish there are.

MR. GROMAN: Pete, do you agree with that?

MR. WELLBORN: I do right now, but what's scary is that going back to a theme of technology one-upmanship, if you go back to the Sanford Wallace days, you had to be an internet rocket scientist to figure how to pop these e-mails out, and even then you're doing it at a rate of thousands a day. Nowadays you've got script kiddies, you've got people who can barely log on that download this software, follow the idiot-proof directions and those people are popping out a million e-mails a day. And when you do the math, it's staggering, not even look at a honed reputation.

MR. GROMAN: So, is that a way of saying probably not just 150 people?

(Laughter).

MR. WELLBORN: I'm saying right now possibly

yes, but if we don't do something, it's going to be -- that the number of awful, awful Spammers is going to grow.

(Applause).

MR. GROMAN: Okay. So, while we're on the topic of big ISPs, we've heard that -- it happened on -- this Monday, AOL, Yahoo and Microsoft announced that they're going to have increased coordinated efforts with law enforcement to enhance enforcement efforts against Spammers. My question to Paula and Stephen is what is it that you want to see AOL, Yahoo and Microsoft do to help both of you do your jobs.

MS. SELIS: Well, having had some experience in our own backyard with Microsoft and some very good cooperation, I'd like to see them and other ISPs take action and sue more Spammers. I think that would be a huge step and a step in the right direction. Also, information sharing, at least in Washington we have a data base of Spam complaints, sort of a mini FTC data base from Washington residents. And we would share that information with the ISPs so that they could use it to target Spammers. In turn, if there were a case or a particular Spammer who they thought would be best served by a state lawsuit, we would like to be able to take that. So, I think there is a lot of room for

cooperation.

MR. GROMAN: Stephen?

MR. KLINE: I haven't run into any problems with the three of them. I think the intelligence-sharing, which we've started, has been unbelievably helpful. And, you know, every time our name winds up in the paper for a MonsterHut or something, we always wind up with 20 phone calls, some of them anonymous, some not so anonymous, saying well, there's five other Spammers, and here's some information.

You know, I would encourage not just the big ISPs, but the smaller ISPs, and any other sys-admin out there who has information on this, to pick up the phone and call your local AG. And if your local AG doesn't seem that up on the issues, sit down and educate them, you know? You know, we're not going to know as much as a sys-admin, but we're happy to be educated about it. And that's where the good cases are going to come from.

MR. GROMAN: We followed the international panel, and in my conversations with all of you before this panel, you all mentioned that you encounter concerns and challenges in the international arena. So, what are the issues as litigators that you're facing in terms of international issues. I'll start with you, Pete.

MR. WELLBORN: I knew you were going to start

with me, because I told you just to skip me on that question before we started that panel.

(Laughter).

MR. WELLBORN: And I'll speak very honestly. When an international issue is figured in, that can make the case and the discovery and the investigation a horrible pain in the rear. The best thing to do, it goes back to what we said earlier, which is follow the money, because if you have a Spammer from whatever-stan, chances are that Spam is not asking you to mail your check to some small town in whatever-stan. Instead, that's either a third-party relay, where the operation truly is in the U.S. or if it's especially sophisticated, it's a foreign mailer for a U.S. company. So, the first thing I do when I see any kind of indicia of foreign involvement is redouble my efforts to follow the money, and nine times out of ten, if not higher, I'll confirm that, hey, that was just a smoke screen, this is a guy down in Florida, or this is a guy up in New York.

MR. GROMAN: Would you be less inclined to file a case if you know there's a large international component?

MR. WELLBORN: I would not be less inclined, but I would steel myself for the battle.

MR. GROMAN: Jon?

MR. PRAED: International is a major problem, and it's a growing problem. But, again, it's not a problem that's unique to Spam. I don't think it should deter Spam litigation, but you do have to plan for it. And one large thought, obviously there needs to be coordination, international coordination, and I know that that's happening, in large part with the FTC's help. And I applaud that, that international coordination.

I think, though, there's a technological coordination, as well, which involves providing the individual consumer the ability to tell their browser or their mail service that they want to respect geo-political boundaries and literally tell their browser I do not want you to take me to websites that are hosted in the former Soviet states. Right now, that is not technologically possible very easily, certainly not by the average consumer, and it's something that the consumer, I think, would applaud being provided that sort of empowerment.

MR. GROMAN: Dietrich, anything on the international front in your cases?

MR. BIEMILLER: We tend to figure that into the low-hanging fruit analysis and avoid them when possible.

MR. GROMAN: Paula?

MS. SELIS: I'll have to echo Dietrich on that.

It's very difficult using state resources to handle a foreign aspect to a case.

MR. GROMAN: Stephen?

MR. KLINE: I would have to echo that, as well. We did have a foreign aspect in the MonsterHut case, Gary Hartle, the technician that we sued was living in Canada, I think did most of his work from Canada, his non-MonsterHut work. When he heard -- we got a little lucky with a dumb defendant, because when he heard that we were looking for him, he called us and --

MR. GROMAN: That makes it easy.

MR. KLINE: -- asked us if he could -- if we could go to his attorney's office in Niagara Falls to serve him in front of his attorney, rather than coming up to Canada, and we said of course you can come back to the U.S.

(Laughter).

MR. KLINE: You know, I'm not so scared of the international aspect anymore, I guess.

(Laughter).

MR. KLINE: But generally, yeah, it -- the second we see it go to another country, the process for us is such a laborious one and such a time-consuming one that we really have to consider whether that's the best use of our resources.

MR. PRAED: Marc, if I can, I'd -- anyone who wants a good primer on how complex the international arena can be, AOL in the CN Productions case moved for contempt against the defendants after having gotten a judgment against them. They continued to send Spam, and we brought a motion for contempt and were ultimately successful in that. AOL on its legal website has a lengthy brief that explains the factual scenario behind what was an international conspiracy. And I think the facts would be -- it's a fascinating reading for people who are really interested in that aspect of the Spam fight.

MR. GROMAN: My last question for each of you, before I open this up to the audience, is what is the greatest challenge ahead, the greatest practical challenge ahead, in terms of Spam litigation? Stephen?

MR. KLINE: Manpower. It is tough trying to justify spending so much time and energy on a case where we're not getting any money back to consumers and the money for penalties isn't there and, you know, we get an injunction and they flee the country. So, it's --

MR. GROMAN: Resources.

MR. KLINE: Yeah, resources really is just the toughest part.

MR. GROMAN: Paula?

MS. SELIS: I'd have to agree with that. I think resources and I think that the potential challenge is bad Federal law, I'm hoping that we don't face that. But given our current status, I think the biggest challenge is resources, the technical savvy, the people and the money to actually take these cases forward and win and to make it justifiable in the end.

MR. GROMAN: Dietrich, your thoughts?

MR. BIEMILLER: I can pretty much echo both of those things, even just from a small private side, trying to match up the resources and then the collections end on the other end. That's going to be a tough connect on some of these cases.

MR. GROMAN: Jon?

MR. PRAED: I'd echo that. Resources, and I think on a longer term, eventually the real hard-core fraud-Spam problem is going to be solved, I think, in the next couple of years. Then we'll be left with a low-level threshold of Spam, largely coming from young teenage boys. And I think our challenge as a nation, to be honest, is to find some way to engage some very sharp, young people, so that they can be challenged in a way that is fruitful. And dealing with that and finding a way to collectively do it, I think, is quite honestly our biggest challenge.

MR. GROMAN: Pete, you get the last word.

MR. WELLBORN: I think the biggest challenge is to generally deter the number of Spammers, because the technology, as it increases, puts so much power to do bad in the hands of so many people who don't have to be rocket scientists. We talked about a Whack-a-Mole idea, we need to take some Whack-a-Moles, and after we whack them, draw them, quarter them, put their head on a spike and parade that in front of the other Spammers.

(Laughter).

MR. WELLBORN: We really do need to send a message.

(Applause).

MR. GROMAN: On that colorful note, would anyone care to ask any of these trial attorneys questions? Where are the microphones? Okay, right up here in the front, the gentleman on the end. Please identify yourself and wait for the microphone.

MR. TYNAN: Dan Tynan, PC World Magazine. You guys have talked about Spammers engaging in fraud, in forgery, in hiding money off-shore, pump-and-dump schemes, a lot of pretty serious criminal activities. Have any of you in your investigations uncovered links to organized crime, and if so, would the RICO statutes apply?

MR. GROMAN: Why don't we start with the AGs.

MS. SELIS: No.

(Laughter).

MS. SELIS: New York is bigger; you go first.

MR. KLINE: You know, we've only had one case publicly, and anything that's pending, we couldn't confirm or deny. But I wouldn't be surprised if you started seeing money pop up in places like that.

MS. SELIS: Ooh.

(Laughter).

MS. SELIS: Well, we have not thus far seen any links with organized crime, but you bring up something, which is that apart from the Spam we oftentimes see an underlying scheme that we find problematic, you know, a get-rich-quick scheme or a wonder drug or something like that. And when we bring our cases, we not only file against them for purposes of violating our Spam statute, but we also allege that they're violating our consumer protection act by making misrepresentations, which isn't quite a crime, but it's a sort of similar kind of activity.

MR. KLINE: You know, I think there's one similar example. I think any time that there is an easy way, a shady way, to make money, organized crime is going to start to find their way into it. A perfect example of

that is a case I handled with the FTC against Crescent Publishing. We -- there was $300 million worth of credit card fraud for -- through adult websites just -- I want to say a month ago, a month and a half ago. The Eastern District of New York and the U.S. Attorney's Office in the Eastern District of New York indicted Bruce Chew and two others involved for laundering money and kicking back about $8 million to the Gambino family, was it? Yeah.

MR. GROMAN: Next question. The lady over here with the glasses, please.

MS. BECKER: Francois Becker from L-Soft International. If you're a legitimate list operator with double opt-in and everything, what kind of information do you need to keep on each of your subscriptions to protect yourself from frivolous lawsuits by people who subscribe and then claim you Spammed them?

MR. GROMAN: Do you want to pick a lawyer to answer that? Anyone want to handle that one?

MR. WELLBORN: I'll take it. The most obvious information in relation to the three-way handshake that you allude to, which is a means of confirming someone's opt-in, it's to keep false opt-ins -- if I wanted to really get back at one of ya'll, I could go to all these different sites and opt-in your e-mail address and then suddenly you're getting flooded with Spam.

To prevent those false opt-ins, there's something called a three-way handshake where the list or the mailer to whom that e-mail address is opted does not just start Spamming, an e-mail is then sent to that person that says someone opted you in, we think this was you, if you do not reply to this, you'll never hear from us again. If it really was you, reply back. And, so, you actually have the reply coming from the e-mail address that was opted in. So, I'd say first and foremost, keep all information available, logs, everything, about each aspect of that three-way handshake.

MS. BECKER: But you've got millions --

MR. GROMAN: Do you need a microphone?

MS. BECKER: If you have millions of subscribers throughout many lists -- if you have millions of subscribers, you're still saying we need to keep every single e-mail, or is it enough to have the IP address that the okay came from?

MR. WELLBORN: I would keep

AUDIENCE MEMBER: (Inaudible) -- I mean, there's a cost to doing business.

MR. WELLBORN: I would say definitely keep every bit of the transaction, because especially -- my radar goes up, when people start talking about opt-in

lists with millions of people --

MS. BECKER: We've got hundreds of thousands of lists, each of them -- I run an epilepsy support list, 500 people. We've got a site that has --

MR. GROMAN: Keep the follow-up very short, please.

MS. BECKER: We've got 200 cancer lists. There's a lot of people with cancer, and there are cancer support people. And we've got volunteers operating these. We don't have -- this isn't necessarily a money-making thing for some of them.

MR. WELLBORN: With the cost of storage, save all you can and you also have an important factor, a different conversation for a different time. I'm not sure you all are commercial, based on what you just said right now, so the rules are a little bit different for non-commercial activities.

MR. GROMAN: Okay, we'll move to the next question. Do we have any questions from the internet? Okay, any other questions from the audience here? Can we have the gentleman over here, please? Please identify yourself.

MR. GELLER: Hi, my name is Tom Geller from Spamcon Foundation. And my question is for all of the attorneys, especially the trial attorneys. How do you

manage consumer demand for your services? At Spamcon Foundation, we don't actually address individual Spam issues, but it doesn't stop dozens and dozens of people every week writing to us saying I received this Spam, can you help me out, can you figure this out for me. And I'm just assuming that it's similar for you folks.

MR. GROMAN: Paula, what do you do? You must get thousands and thousands of e-mails in your data base, consumer complaints. What do you do with them and how do you pick the case?

MS. SELIS: Okay, good question, good question.

MR. GROMAN: And I hope I paraphrased that okay for you.

MS. SELIS: A good example, just recently, there were 1,700 complaints during February of this year, so that gives you kind of an idea of the volume. And we're very lucky, we have a website that we put a lot of consumer education material on, tell people how to file their own private actions if they want to. But we can't handle each and every one individually; we can't file a lawsuit on behalf of them all.

So, what we do is we give them the consumer education materials. We have them file a complaint on-line, which enables them to cut and paste their Spam complaint onto the computer itself, and we keep a data

base of that. And then we periodically look at what's in our data base, having already given the consumer his or her education and decide, based on what we find, what would be a good case for us to bring.

MR. GROMAN: Does anyone else want to field that question?

Okay, let's move on. In the back, with the Spam hat.

(Laughter).

MR. GROMAN: We had to go there, right?

MR. FERGUSON: Jim Ferguson, I'm not spews (phonetic).

(Laughter).

MR. FERGUSON: What about the opposite side of the house where the Spammers are suing the anti-Spammers because we're denying them access to our personal inboxes, as well as our networks?

MR. GROMAN: If someone would like to take that, I'd like you to keep that brief. It's slightly off topic --

MR. WELLBORN: I'll keep it real brief. To the extent you're alluding to any particular case, since it's a business entity that was formed just a couple of weeks ago, two months ago, we don't know who it's composed of, but if there's an entity that's composed of Spammers, and

by Spammers I mean people sending unsolicited commercial e-mail into computer networks that they know forbid unsolicited commercial e-mail, those people are criminals, and for them to file suit is analogous to a burglar suing you because you put a lock on your door.

(Laughter).

MR. GROMAN: The gentleman in the back by the door, please.

MR. CROCKER: Hi, Dave Crocker, Brandenburg Networking. First of all, I'd like to thank you all for a great amount of candor, no matter how disconcerting it might be. It helps bring some reality to the expectations about legal enforcement of all this. And that ended up highlighting two disparities that I'd like to pursue. One I want to highlight and one I want to ask about.

The one I want to highlight is the comment about geographic boundaries and any expectation that we're going to be able to tell browsers, oh, just don't go to that country. And it was said that it's not something you could do now. I will tell you, I don't know how to do that, and I ought to, and I don't know how to do that. So, I think that any expectation that browsers are going to be able to do that any time in the near future, like 10 or 15 years, is pretty small.

The other disconcerting -- or disconnect that I'd like to ask about and get some feedback on is we have for most of this workshop been hearing about the high expectations that are held for passing laws and having a strong effect on Spam. And I would say that your consensus sounds an awful lot like that ain't going to happen, and would like you to speak to that some, please.

MR. GROMAN: Do you want to pick somebody? Who wants to field it?

MR. PRAED: I don't want to field that portion of the question, but I want to field -- we've been to the moon. We can certainly teach internet browsers how not to go to former Soviet states or to the Bahamians, the Bahamian Islands.

MR. GROMAN: Okay, the part of the question about is this legislation really going to do anything? Or are we kidding ourselves?

MR. CROCKER: My background's technical. When I said this, we haven't taught anybody how to stop war. There are lots of things we can't do. There are physical limits in this world.

MR. GROMAN: Okay, I want to stick to the issue of litigation and legislation, off the browser topic. Anyone want to give an opinion, as a litigator, if we have legislation that wants or seeks to encourage

litigation or law enforcement, are we going to see anything happen?

MR. WELLBORN: As far as the legislative end of things, if we have a law that tightens the noose, I'm all for that. If we have a law that arguably or purports to legalize that which is illegal right now, I'm against that, and in fact, it would be a bad Constitutional problem because an ISP's right to regulate how its computers are used, that's one stick in its bundle of property rights.

And, so, if you have any situation where the government comes in and says, ISP, you can no longer sue under common law trespass, you can no longer say that people can't send unsolicited commercial e-mail through your network, if that were to happen, there'd be serious Constitutional issues. Right now, even without the Spam-specific laws, which we would all love one if it had teeth and it were good, but even without that, our gun's already loaded with about a dozen or so bullets, any one of which will get the Spammer.

MR. GROMAN: Okay, next question. Gentleman in the back row.

MR. BERLIND: Hi, David Berlind with CNET. And to Paul Wellborn's last point that drew quite a bit of reaction from the audience, which is we should draw and

quarter Spammers, my question is, you know, we watched the news recently, now that the war is over, the news is going to other things, and one of the big focuses now is how none of these people who have run afoul of good corporate governance haven't gone to jail yet.

And the question here is, you know, I think a lot of people believe that in the world of Spamming, assets can be hidden and financial penalties are kind of worthless, but if we make examples of a few people and put them in jail that might change things, because you can't hide the body. You can hide the money, but you can't hide your own body, and so, what is it going to take to improve the punishment from the recipient's point of view to make a few examples here so that Spammers do really think twice because the punishment is much more serious than something that they can --

MR. GROMAN: Is the question do we need a bigger punishment?

MR. BERLIN: Sure.

MR. GROMAN: Anyone want to field that?

MR. WELLBORN: I hate to take every question. Make me prosecutor for a day, I'll put them all in jail.

(Laughter).

MR. GROMAN: Okay, we have a question up here, please. Right up here in the front row.

MR. KELLY: Hi, Ben Kelly, Attorney in Los Angeles. I have a quick question for probably mostly the litigators here. What has been -- what are your thoughts or what have your experiences been with a would-be Spam plaintiff's duty to mitigate?

MR. PRAED: I'll take that. Obviously duty to mitigate is a standard requirement. I think most of my clients in my experience have fully discharged that duty and are doing everything they can both to filter and to put Spammers on notice. I think the Verizon Online versus Ralsky case really stood for the principle that no professional Spammer today can realistically say that they don't know that what they're doing is in violation of what Pete so eloquently points out is one of the most important bundles in the bundles of sticks that we all have, the right to exclude others from our private property. Duty to mitigate is not a new concept. Plaintiffs generally meet that duty fairly easily.

MR. GROMAN: I want to return to an earlier question and give our former assistant district attorney an opportunity to address that question about increased penalties. Stephen:

MR. KLINE: You know, I agree with Pete that if a few of them were in jail it would be tougher for them to Spam. The problem that we have, and we have secondary

criminal jurisdiction in New York, is the same sort of problem we have on the civil side, and that is, you know, for all the resources we have, if I marched into my boss' office and said you wouldn't believe this guy is sending billions and billions of e-mails every day, and it's costing this large corporation a lot of money, and on the other side there's another assistant saying and over here we've got people who are creating false passports for terrorists, they're laundering money through Aholla's back to Pakistan and all of this, I can tell you who's leaving the office first and looking for another case.

(Laughter).

MR. KLINE: And I think Pete would agree. We've talked about this a little. As much as we despise Spammers, I'd much rather see a pedophile or a terrorist taking up that jail space than a Spammer.

MR. WELLBORN: As would I.

MR. PRAED: Just a quick comment. I think, though, what we're seeing is an exploitation of what in the end is a systematic problem, and I think Spammers are taking advantage of those same exploits that terrorists, quite frankly, are taking advantage of. And to the extent that we're -- to some sense and some degree it doesn't matter who you chase, as long as you are chasing someone who is taking advantage of that exploitation and

close the loophole. You're going to fix both problems.

MR. GROMAN: Okay, let's move on to another question. The lady up front please, in the white.

MS. ANGWEN: Hi, Julia Angwen (phonetic) of the Wall Street Journal. On the same note of increased penalties, I'm just wondering why, if some of these Spammers are using stolen credit cards and engaging in fraudulent marketing, why hasn't there been any criminal prosecution of them?

MS. SELIS: Well, I have to come back to what Stephen was saying in terms of resources. There are a lot of potential criminal cases out there, and when you are facing, you know, property crimes versus physical crimes versus terrorism and you have to choose among them because you have limited resources, what oftentimes happens is that you're going to go to the more serious crimes first. And of course that's a philosophical question as to what is the most serious one, but oftentimes it's the one where there involved some sort of bodily crime.

The Washington AG's Office does not have criminal jurisdiction, but we do try to look at the underlying issues. So, for example, if there is credit card fraud or if there is a misrepresentation going on, we may refer something out to the prosecutor. And there

is a question as to whether the prosecutor is going to take it or not. I can speak in the off-line world, where we have had just generic consumer protection cases that have involved identity theft or fraud, and I have referred some of those cases to our prosecutor and sometimes the prosecutor will take them, if they involve enough dollar loss, and sometimes our prosecutor will not. So, it really comes down to resources once again.

MR. GROMAN: I also want to point out in response to that question if you have a Spammer who is engaged in Spam but is also engaged in identity theft or credit card fraud or some other criminal behavior, that individual may very well have been prosecuted criminally, it's just not a Spam case necessarily. So, maybe they did go to jail for the other behavior, but it wasn't a Spam case under the Washington AG Spam statute.

So, I don't want to leave the idea that these people aren't being prosecuted; they very well maybe, it's just that it's not a Spam case then, it's a different criminal action.

Yeah, I'll take a question from the gentleman in the back, please.

AUDIENCE MEMBER: How do I go on notice saying that I don't want Spam sent to my domains? I'm not an ISP or anything. To whom do we send the check so that

the AGs can go to their bosses and say people are willing to pay for this?

MR. GROMAN: The IRS.

(Laughter).

AUDIENCE MEMBER: But the IRS doesn't know that I'm sending that check for this purpose. And can we create automated tools that facilitate the tracing of who it is that's sending the Spam so that it provides easier ways for the AGs and attorneys to figure out who to go after?

MR. GROMAN: The question's about automated tracing.

AUDIENCE MEMBER: Yes, the question is is -- you know, can we create Spam bait out there like honeypots are doing and things like that to try to go and trace back who the Spammers are, so that the information is gathered, held onto and traced back and tools for figuring out --

MR. GROMAN: Well, I think that the next panel actually is going to address some technical issues, so let's keep this to litigation, and we'll leave that to the next panel.

If we could have the gentleman in the back, right behind you, please.

MR. SILVER: Hey, my name is David Silver.

Pete, I have a quick question for you just real quick. You had made a comment to a lady's question earlier about, you know, the kind of information that needs to be kept in order to prove whether you've not done Spam or not. So, just a point of clarification, so companies that may be not practicing double opt-in, are they at risk of being -- having a lawsuit filed against them? Because I think this question of what attributes are required to be kept is really important for lots of large corporations that are trying to identify how do they fight -- or keep from being sued as a result of what attributes are required to be kept. And many companies don't do double opt-in. So, I just have a question for you, are they open to a lawsuit as a result of not having that information?

MR. GROMAN: And you can send a bill for legal services when you answer that.

MR. WELLBORN: Oh, that's a great question, and it reminds me of an old contracts professor I had in law school. He would say you can sue the bishop of Boston for bastardy, but you might not win.

(Laughter).

MR. WELLBORN: And what that means is that might you get sued? Yes, certainly. If someone falsely opts in an e-mail address and there's no three-way

handshake to confirm that e-mail address, might that person get mad and sue. Yeah. Would your client possibly win because they had no way of knowing or they weren't one of these outfits that's in the business of taking false opt-ins, you know, yes, but the key factor there -- I would advise one of my clients to not think about what lets you win the lawsuit but instead think about what lets you avoid the lawsuit altogether.

MR. GROMAN: Next question? We're going to go all the way into the back corner. And please identify yourself before your question.

MR. LEVINE: I'm John Levine from CAUCE Abuse Net, and I have sort of a question and a half about private right of action.

MR. GROMAN: Well, we're almost out of time, so if we can keep it quick, please.

MR. LEVINE: The junk fax law is primarily enforced by private right of action. Two things to make it hard is it's complicated to explain to small claims judges who frequently don't have a lot of real training, and the other is that small claims have to be filed in the defendant's location, which with faxes is frequently the same as yours but with Spam never is. I'm wondering, is there anything we could do to make PROA more enforceable for small plaintiffs who have received Spam.

MR. GROMAN: Dietrich, that would be you, private right of action.

MR. BIEMILLER: Well, I think the jurisdictional issue is one -- I've got one case right now that was brought in small claims court and the defendant appeared over the phone, so it's really not that much of a hurdle for them to actually appear in court from anywhere in the world. Again, the enforcement of that is going to be difficult, but -- and as far as the junk fax thing goes, it's more of tracking down who the real Spammer is and it's something that anyone can do if they can find -- through vicarious liability theories where the money's going and then, you know, go against that person. Does that answer your question?

MR. GROMAN: Paula wants a word on that.

MS. SELIS: Just to follow up on that one, in Washington, small claims courts are courts of limited jurisdiction, and they define themselves by statute. And one of the ways that they define themselves is that they say that you can't bring an out-of-state defendant into small claims court. Yeah, I think it's very common. But you can bring an out-of-state Spam defendant into district court, which is very similar to small claims court. The filing fees are very low, pretty simple procedures.

So, I think it's going to vary from state to state, jurisdiction to jurisdiction, whether you can haul somebody into small claims court or not. But it is an issue, and it was an issue in Washington, and as Dietrich pointed out, we clarified in our statute, just this last session, that you could at least bring an out-of-state Spammer into district court.

MR. GROMAN: Okay, I'm looking at a lot of glazed faces that appear desperate for caffeine.

(Laughter).

MR. GROMAN: So, I want to thank the panelists. Before we close, I do want to mention that the Chairman made -- mentioned in his opening remarks that the Federal Trade Commission, along with state law enforcement and other federal agencies, are going to be announcing on May 15th some new law enforcement actions that will address on-line fraud and Spam. And that will be following up some of the things we've talked about at this forum.

So, on that note again, thank you very much to our panelists and we'll see you back.

(A brief recess was taken).

MR. HUSEMAN: Good afternoon. We're finally here for the last panel of three days. And my name is Brian Huseman. I'm a Staff Attorney with the FTC's Division of Marketing Practices. And I just asked who

gave me this lousy time slot, but I guess that was me, so I guess I can't complain.

(Laughter).

MR. HUSEMAN: In this panel, we're going to be talking about two very distinct things but two very important topics in our solutions day. We'll be talking about technological solutions to Spam and also structural changes to e-mail. I really see the panel delving into three different phases, and the first will be what current technological approaches can we use to try to solve the Spam problem. And I want this panel not to be a discussion of should someone -- should a consumer or a business buy Spam product A versus Spam product B. That's not a very useful discussion. Instead, we're going to be focused more on the technologies and the approaches themselves, what are the pros and cons of each of these different methods of dealing with Spam in a technical manner.

The second phase of the panel will be talking about some specific panels that have been put forth about how we can, with technology, deal with the Spam problem. And then the third phase we'll be talking about some big picture structural changes to e-mail, the way that the e-mail protocol is set up, the way that we communicate with e-mail. And, so, we'll be just tossing some of these

ideas out there and evaluating whether they're efficient or even possible to do.

This is one area where the FTC, you know, does not have a lot of expertise in, as we're not technologists, we're lawyers instead, but it is probably one of the most important, if not the most important, possible solution to the Spam problem.

And I want to point out initially before we start that Ira Rubinstein from Microsoft has been replaced by Ryan Hamlin here on my far right, who is the general manager of the Anti-Spam Technology and Strategy Group at Microsoft, so just make that in your notes.

So, we're first going to start out with John Levine. John, will you please show us your presentation? We're going to -- get us all on the same playing field. And I would ask all the panelists, you know, as I said, I'm a lawyer, not a technologist. John is the author of "Internet for Dummies," so that's a good approach and mindset to keep in mind. Let's talk about this from a dummy's perspective at the beginning to examine the various approaches and the pros and cons of each.

MR. LEVINE: Thank you, Brian. I'm going -- I have set for myself the simple task of explaining all known approaches to Spam filtering in four minutes, which is not going to happen. But my goal in this little pitch

is basically to show you that there's a lot of different approaches that have already been attempted and are already fairly well understood and that people keep reinventing, because there's a very bad habit for people to think that they're the first person ever to invent the idea of a white list or something.

So, if we can categorize the approaches, I think it makes it much more -- it will make it much easier to talk about what's promising and what's not promising. And I will attempt to keep my snide remarks about the promisingness of each approach to a minimum.

As we move through sort of the stages of processing an e-mail, the first is source filtering, looking at where -- even before you receive the message, looking at where it comes from and how do you decide whether you even want to accept it in the first place. And I have five approaches here. I'm going to explain these very fast, and if you don't understand everything, come and talk to me later, and I'll be happy to tell you in more detail when I can talk slower.

The first couple of lists are blacklists. There's a variety of ways that people create blacklists. The first one is mechanical, mechanically generated DNS blacklists. These are things that report -- things that you can test mechanically that are known to be sources of

Spam, open relays, proxies, addresses that have sent to Spam-trap addresses.

The second category of blocking lists is what I call untrustworthy senders. If a machine is a dial-up user of a consumer ISP, a correctly configured mail system will route the mail through the ISP's mail server. If it attempts to send directly, it means it's either a Linux weenie or it's a Spammer. And Linux weenies are educable, so in general, it makes sense to reject that kind of mail.

The third kind of blocklists is what we call shared reports. A lot of people send in reports that they're Spam and based on those reports, it more or less automatically creates a blocklist of the addresses from which the reported Spams came.

The next kind of blocking lists are waiting services, Spam sources. These are actually created by human beings who are identifying sources that they believe are sources of Spam or related to Spam, that you probably wouldn't want to receive. And the best known are the SBL and the MAPS RBL, both about which we heard quite a lot yesterday.

And the final source filtering scheme is what I refer to as DNS poisoning, which is basically to say if -- when an incoming message has a return address or a lot

of domains that appear to send nothing but Spam, and if you simply adjust the mechanics of your internal domain server so those domains can't be found, then your normal reject scheme that rejects mail with impossible senders will reject it.

The other kind of poisoning is simply -- if you notice that there are Spammers on a particular network, you can adjust your own domain server so that when they send a request to you to say where do I deliver mail for your domain, it sends back a message saying I don't know, which is -- it's not widely used, but it's quite clever.

Once the message is received, now there's a whole bunch of approaches to content filtering, where you actually look at the message to decide whether or not you want to receive it. The first is protocol defects. There's a mechanical definition of the SMTP protocol, and in general, the legitimate software does SMTP correctly and the more defects in the transaction, the more likely it is that it's sloppily written Spamware.

MR. HUSEMAN: John, what is SMTP?

MR. LEVINE: Oh, it's the optimistically named simple mail transport protocol. It's the scheme used to transport mail from one computer to another over the internet. Sorry.

So, first -- again, you can make these fairly

mechanical tests, and these are quite reliable. The next is look at the headers of the message, and this is where you come into sender white lists and black lists. If it's from a sender that you know you don't like, you reject it; if it's from a sender that you know you do like, you accept it. And there also turn out to be other kinds of mechanical defects in the headers that you can check for, and again, the more defects you have, the more likely it is that it's Spam.

MR. HUSEMAN: John, can we go back to your first protocol defects. What is RDNS?

MR. LEVINE: RDNS is the reverse lookup to find out where the message came from.

MR. HUSEMAN: So, can you give us an example of how that would work?

MR. LEVINE: Yeah, whenever a message comes in, it has, as we saw in the session on the first -- in Nick Nicholas' session in the first day, it has a sender -- it has an address it's routed to and it has a return address. And the return -- what you can do is you can simply look up the return address and say, where would I deliver mail sent back to that return address. And if you don't get a response, you know the return address is forged, and that's a very strong indicator that it's Spam. And, again, my previous thing about DNS poisoning

basically makes it look like your own addresses are forged to confuse Spammers.

Once you've analyzed the headers, there's various things you can look for in there. Then I think the largest category of Spam filters are body strings. They actually look for pieces of text in the body of the message. These slides are all on my website. I can give you the URL later, so you don't have to carefully copy them all down.

There's two kinds of body filters. One are what I call fixed body filters, where the strings are more or less built into the filtering program or they're updated occasionally. The other is what I call adaptive body filtering, which is also known more trendily as Bayesian body filtering, where you simply say here's a whole bunch of Spam, here's a whole bunch of non-Spam, and it uses statistical methods to try and figure out what strings are likely to appear in Spam, what strings are likely not to appear in Spam.

Bayesian filtering used to work really well. But since Spammers are not totally stupid, they have figured out to make their Spam look either -- either look more like real mail or to be so short that there aren't enough strings to apply filters to.

MR. HUSEMAN: John, so Bayesian filtering,

would that be, for example, the same -- if a Spam message has the words free plus money plus offer, then there is an X percent chance that that is actually Spam message?

MR. LEVINE: Like that except that it's completely automated by software. You simply say here's all my Spam, here's all my real mail, and it figures out what those likely strings are. And having looked at some of the Bayesian filters that have been generated automatically, they come up with wild stuff, stuff that you wouldn't expect, which frequently turns out for a while at least to be a really good indicator of Spam, at least until the Spam mutates.

The next that I find works really well is bulk counting. I use a system called DCC, called short for distributed checks on clearinghouse, where basically what it does is it makes sort of a one-line code number that digests the content of each message. And then a group of DCC servers simply go and count the number of messages with the same signature. And if you have many messages with the same signature and they're not from a known good mailing list, it's probably Spam.

Again, I find this extremely effective, particularly I have a lot of e-mail addresses that appear in my books, so they never -- they absolutely cannot legitimately subscribe to any sort of real mailing list,

so any bulk mail that comes to those addresses must be Spam. And bulk counting works really well for that.

A related thing is what I called shared announcements, where DCC simply counts -- DCC counts all the messages, and you have to make special arrangements for it not to look at your legitimate mailing list. Shared announcements, the best known of wish is Vipol's Razor, which has been commercialized as Cloudmark. People send in their Spam, and it attempts to come up with a shared counting system for just counting Spam, not counting all the messages.

MR. HUSEMAN: So, John, can you give an example of how that would work practically?

MR. LEVINE: Oh, people basically, when they're going through their mailbox, every time they see Spam, they forward it off to the local Razor server. And then it automatically updates the bulk counters that it keeps, so that when future mail comes in, it can say, oh, look, this has the same signature as all these messages that were reported as Spam, therefore it's probably Spam, too.

MR. HUSEMAN: So, is this also known as the peer-to-peer or collaborative approaches --

MR. LEVINE: It's one of the collaborative approaches. DCC is also collaborative. The difference is that DCC is automatic. It counts everything, and you

have to separately figure out what's from a real mailing list.

MR. HUSEMAN: Does DCC stand for something?

MR. LEVINE: Distributed checks on clearinghouse. It's a tool beloved by weenies.

(Laughter).

MR. LEVINE: It's hard to install and hard to explain, but it works really well.

(Laughter).

MR. LEVINE: Razor particularly in its commercialized form is easier to set up because it's been packaged in a more attractive way.

And, finally, what I can only call Spammy behavior, if you have like subject lines with random strings of text and numbers in them and e-mail messages -- you know, I get a lot of e-mail messages that start with sort of long sets of words that clearly mean nothing. Those are called hash busters. Those are specifically put in there to defeat these bulk counting systems, to try to make all the different copies of the Spam look different enough that they're not recognized as the same. However, you can look for hash. There's a lot of hash busters that turn out to be done in really dumb ways, and you can count them and you can identify them.

The next approach is hybrid filtering. No

single approach works all that well, so we mix them and match them. Some of the best known are Spam Assassin and Mail Shield. I happen to use Spam Assassin because it's free and it runs on the kind of server I use. And there are lots of add-ons to your mail transport agent, the actual mail server software, that you can buy. And I think if you talk to most ISPs, they will -- at least part of their Spam filtering will be home brew, so there's a lot of variation there, too.

Now, this next thing starts to approach on ways that we might be changing the way that e-mail works. And sender identification is a way to say that if we know who the sender is and we know it's not somebody we hate, then the mail is most likely good. The best known sender identification are the two cryptographic signature schemes, PGP and S/MIME. They work pretty well, but the fact that they've both been around for years and nobody uses them suggests that they have usability problems.

The next possibility is what I call per-correspondent addresses, and there was a blurb out there for one variation, a blurb out in the back, for one variation of this. And basically you give each of your correspondents a different address of yours to send mail to. And then if -- when the mail comes in, if the address it's sent to matches the correspondent you gave

it to, you know it's okay. If it comes in to some random other address, or even worse, if you get mail that you gave to person A, but you received mail to that address from person B, that suggests that they sold or transferred your address.

So, that can be a very good way to keep track, particularly when you're doing business with companies, all of whom require an e-mail address. It's a good way to keep track of who you're corresponding with. And in my case, I find it's very useful that a message shows up in my inbox and I say ooh, it looks like Spam, and then I say oh, wait, that's the right address, I did business with them a year ago, so I know it's okay.

MR. HUSEMAN: So, would this be a disposable e-mail address?

MR. LEVINE: You can treat them as disposable. In my case, they're not disposable; either they're active or they go to the Spam trap. But other people treat them as disposable.

A related thing to this, actually to the reverse DNS lookup is some mail systems actually when an incoming message comes in from an unfamiliar address, it actually starts a session back to the sending mail system and attempts to deliver -- it goes through the first half of an SMTP session to try and send mail back to that

address, to see whether at least the address is accepted. And this is a more sophisticated way to validate that the from address is real. This isn't widely used, and I think this has scaling problems. I think it would be really resource-intensive to use a lot.

Another popular scheme that I don't like for reasons that I won't take time to explain is challenge response. When somebody -- you send mail to someone you haven't heard -- you haven't corresponded with before. And his computer automatically sends back a message saying who the heck are you. And if you respond to the challenge in some satisfactory way, and satisfactory is anything from clicking on a link to sending them an essay explaining why you were worthy of their valuable attention. But if you send back a satisfactory response, then you're white listed.

There are a variety of trusted sender schemes, and Vince is going to tell us about one, so I won't attempt to describe it. But this is basically a way to say that not only can you identify who a message is from, but some organization who you presumably trust says we have investigated the sender and the sender says that this mail is of such and such a category and from our -- as far -- you know -- and we will assert that what he's saying about it is true. So, that can be useful as a way

simply to put useful labels on mail, so that mail can identify itself as yes, this is bulk; yes, this is not bulk. And, so, if they lie about it, it's much clearer -- you have a much clearer way to go after them and say not only is it Spam, but you're a liar.

And the final one in sender identification are various technical ways that are sort of analogous to the realtime mailback but more technically efficient to verify that the address -- that the internet address that a piece of mail is coming from is a sending server that is authorized to send mail with that return address, and it's simply -- it's a more complicated and more sophisticated way to validate that mail is actually coming from who it purports to be coming from.

And, again, it's similar enough to per-correspondent addresses and signatures that we can consider them all together.

MR. HUSEMAN: Now, where would the white list approach fall? Would it be a sender identification method?

MR. LEVINE: I actually treat that more as content filtering, because partly it's -- well, no, white list is not sender identification because you have no way of knowing that the address that the message purports to be coming from is actually who it's coming from. In

other words, you know, if I -- if I know Brian's a good guy and I put his address in my white list, then all mail from you will automatically be white listed. But if some third party then sends me a virus that fakes your address in the return address, it will pass through my white list, even though it's not really from you. So, the point of the sender identification is to distinguish mail that's really from you versus mail that only purports to be from you.

MR. HUSEMAN: So, white list would fall under the content filtering. And if you could briefly explain what a white list is.

MR. LEVINE: Oh, a white list is simply a list of e-mail addresses from which you believe you want to receive mail. I mean, like everybody in this room, I would guess, would qualify for my white list. You know, so if you send me mail, it will basically say oh, it's from you, I'll bypass all those other filters and I'll just put it in my mailbox.

MR. SCHIAVONE: Did you opt in to every mailer in the room?

MR. HUSEMAN: Please speak in the mike.

MR. LEVINE: Did I -- Vince asked did I opt-in to every mailer in the room. For individual messages telling me how wonderful I am, yes.

(Laughter).

MR. LEVINE: And my final set of possible changes to e-mail are what I call -- are postage schemes, ways to put -- basically, some ways to charge the sender some amount for the privilege of delivering mail to you. And they fall into two large categories. One is what's called hash cash, where there's no money involved but the sender -- you present the sender with a computationally difficult computing problem, which it then has to solve to allow the message to be delivered. And the idea is that solving the message will be time-consuming enough that Spamming people will be too slow, because you'll have to solve too many of these problems.

MR. HUSEMAN: Where would that message come from? Would it come from the ISP or from the individual recipient?

MR. LEVINE: Ask six geeks, get six different answers. Some people attempt to send the hash challenge back from the mail server; some attempt to send it back from the end-user. I think that it's not practical simply because the computer speeds vary so much, you know, and my stepmother's 486 might take an hour to solve a problem that a Spammer's two-gigahertz Pentium VI could solve in a tenth of a second. So, I think that makes hash cash impractical.

The final thing is e-postage, where you put real money on it. And I think -- I think e-postage is impractical just because it requires building a brand new organizational structure like the post office, okay? We already have one of those, and it has its problems.

(Laughter).

MR. LEVINE: You know, so everything -- and I say, like, okay, if you're going to charge people two cents to send you mail, that's fine. Now, when a bad guy puts a virus on your machine that sends Spam to third-parties, who pays the postage? I don't know. Yeah, we can probably solve all these problems, but we're going to take one can of worms and replace it with a bigger, uglier, more expensive can of worms. So, e-postage -- everybody says e-postage would be great. I simply don't think that it's implementable.

So, anyway, that's my very short overview. And, again, if you want more detail on what these things are the URL where the slides are, come and talk to me later.

MR. HUSEMAN: Can you just say the URL briefly?

(Laughter).

MR. LEVINE: www.iecc -- that's I E C C -- .com/ftcSpamtech -- T E C H -- .ppt. And if you didn't get that, I'll tell you again later.

MR. HUSEMAN: Thanks. Now, Matt Sarrel, you are technical director for PC Magazine's Internet Lab, and so you have examined all of the actual commercial products, both for consumers and business and tested those out. Let's go through John Levine's categorization of all the various technical approaches to Spam and talk about how those approaches have both pros and cons for consumers and businesses and today's actual products that are out there. What about any source filtering products? What are the pros and cons of that approach?

MR. SARREL: Source filtering works fairly well on a system level. The only -- the immediately noticeable problem to source filtering is when sending systems get placed on blacklists incorrectly, which actually, interestingly enough, happened to Ziff Davis --

MR. HUSEMAN: Which we talked about yesterday, had a sense of discussion kind of about that problem in one of yesterday's panels.

MR. SARREL: So, they can be helpful, but they're not the answer to the whole problem. And they're also, from a computational sense, they're relatively easy to implement and not very costly.

MR. HUSEMAN: What about content filtering? So, this would include various things such as white lists. Let's talk about white lists first. What are the

pros and cons of that approach?

MR. SARREL: I think one of the major pros to white listing is that it's a very easy concept to understand. So, it's sort of like you say this is a list of people that -- for whom I'm willing to accept e-mail, and whatever they send me, I'll accept. Now the problem is, when someone ends up on your white list who doesn't belong there, and the other problem is what happens when you add someone to a white list based on an ambiguous e-mail.

One of the problems that we had in our testing is that the actual definition of Spam, so what's really Spam, what do you really want, what do you really not want. And we happened to get an awful lot of e-mail that we called gray Spam, which is Spam that we didn't ask for, but we read and it turns out to be relatively interesting.

(Laughter).

MR. SARREL: That doesn't happen to everyone, but being in the media, I get e-mail every day from someone I've never met who wants me to look at their product. And if I start rejecting everything that comes from someone I don't know, then that's going to affect my business.

MR. HUSEMAN: Do you think that white lists are

practical for businesses, as opposed to consumers?

MR. SARREL: No, I do not. I think white lists may play a role in the consumer market, primarily because it's very easy to understand. You just put all of the people that you trust already into your white list, and you receive mail and you can look at that. But then you run into the situation of what happens if a long lost friend finds you in some kind of e-mail directory and e-mails you and they're not in your white list. So, then even though you have the white list, you still have to dig through all your quarantined e-mail. The white list is a start. I think actually white lists and blacklists are a start, but they're not an answer.

MR. HUSEMAN: Dan Tynan, you are contributing editor of PC World, and you've also examined the various approaches, technical approaches to Spam, as well as you've also looked at the world of Spamming and some particular Spammers as you described them as well. Let's talk about some more content filtering, and specifically content filtering based upon certain words, their messages. What are the benefits and also the negatives to that type of approach?

MR. TYNAN: Well, I would say that that's kind of been the traditional form of Spam filter for a long time has been content filtering, where it looks for words

like Viagra and worse. We all know what they are. I'd say the sort of the flavor du jour is really white list and challenged response. The last three or four products I've looked at have been exactly that. And that seems to be where the thing is going. I think that's also a response to the fact that content filtering is continually defeated by Spammers.

One example is, you know, a product like Spam Killer. Spam Killer will look for words and phrases. It has something along the lines of 5,000 different content filters. And, so, it will look for the word Viagra, and so Spammers will then put the word Viagra with a little star between each letter, so they have to change the filter. And then they'll put it inside HTML code, and so they'll have to change the filter. And then they'll put an HTML tag in the middle of the word Viagra that's invisible but defeats the filter, and so they have to change the filter. So, it's a constant game of cat and mouse. As a result, my testing, content filters out of the box, 80 to 90 percent effective.

MR. HUSEMAN: And I address this issue, let's say, to John Levine. Is 80 to 90 percent effective filter good enough?

MR. LEVINE: It kind of depends on who you are. If you get ten Spams a week, you know, and it knocked you

down to one, then that's -- you're in pretty good shape. I've had the same e-mail address for ten years, so I get a lot of Spam. And in my case, you know, if my Spam filter is running less than like 98 or 99 percent accurate, I'd have some -- my regular inbox would still have more Spam than regular mail.

MR. HUSEMAN: What about the issue of Spammers using -- or sending a message that has only an HTML image, so there are basically no text words in which to filter? Can these filters solve that problem?

MR. TYNAN: There are some filters that do that look for specific HTML characteristics. Spamnix is one that does that. I think Spam Assassin also does. And, so, they have a waiting system, they assign points and say, okay, if it has this kind of image, then it assigns X number of points. And when it reaches a certain point threshold, it says, okay, this is probably Spam, and it shuttles it off into a Spam folder.

MR. HUSEMAN: What's your response to that, Matt? Do you agree?

MR. SARREL: Oh, with that particular kind of Spam, which is just an HTML image, that's really easy to filter, since no one ever sends you real mail that looks like that. The issue is how hard is it to update your filter to recognize the Spammer gimmick of the week, and

it's more of a software maintenance problem than a technical ability to deal with that particular kind of Spam.

Right now, that's the constant battle, is what's the Spam flavor of the week. Is it V/I/, or is V*I/, or is it Spam sent to me from another country in another language, or is it a graphic. That's -- right now, that's where the war seems to be fought, is can the Spam filtering products keep up with the Spammers.

MR. HUSEMAN: I guess one question I want to pose is that if this is an 80 to 90 percent effective solution, what are the -- first of all, is this solution good enough because of the continual updating and trying to figure out what the new Spammer tactic is.

MR. SARREL: Well, one thing that we did when we looked at these products, we looked at the consumer products and we found them to be roughly between 75 and 85 percent effective. And then we looked at the ISP or corporate products, and they were roughly between 85 and 95 percent effective. And we said well, that's significantly better.

But then if you think about it, if you're -- like John was saying, if you're a consumer and you get 10 Spam messages a day and this software filters them out and now you're only getting two, that's great. But what

if you're an actual company and at this point you're getting 10,000 Spam messages, you know, in a week. So, now what are you filtering out? You still end up with a thousand Spam messages. So, I think it's not necessarily as important to filter out -- the statistics are more interesting than just who's catching the most Spam. It's whether the legitimate mail is making it into your inbox, so in other words, avoiding a false positive, which in a business sense could be very costly. And it's also -- like correctly diagnosing a true Spam..

MR. HUSEMAN: Let's now talk about the technical approach, the collaborate or a peer-to-peer approach. This is where consumers or individuals vote on what they think is Spam and then based upon the aggregate statistics that message is labeled as Spam and then filtered or blocked out. Dan Tynan from PC World, what are the pros and cons to that?

MR. TYNAN: Well, the one that I've used personally is Cloudmark Spamnet and when I started it, it caught about 66 percent of the Spam. And it's one of those products that you have to continually use and tweak and you submit -- you know, you get a piece of Spam, you click on it, you submit it back to Cloudmark, and eventually they develop what they call a trust rating, whether you are a trustworthy sender of actual Spam. And

as your trust rating grows, they give more weight to your submissions. So, eventually they decide that you know what you're talking about and that they will start blocking the Spam for you and for everyone else that you submit. But it takes a while. You know, I didn't test it long enough to really see the improvement. People who were here this morning heard John Patrick on a panel earlier who claimed he had 99.9 percent Spam protection. He uses Cloudmark Spamnet.

MR. HUSEMAN: Ryan Hamlin at Microsoft.

MR. HAMLIN: One comment, we use at Microsoft collaborative filtering, and that's the version that will be shipping now with Outlook and with our next version of MSN. What we like about collaborative filtering is that it's not dependant on a specific set of words, like Viagra, right? There's a bucket of good mail and a bucket of bad mail. And in that bucket of bad mail, maybe the combination M, dash, period, space, space, Y has shown up in many bad mails, and so it's based on that. And, so, it's not as prone as rules-based human error, because it's based on a large sampling of what users identify as good mail versus bad mail.

The key point, too, is that it has to have a mechanism of realtime, because as you know, it's a countermeasure, a battle that we have with the Spammers.

And, so, the nice thing about collaborative filtering, it is near realtime, and so you're constantly training your filters on a frequent basis to react to that Spammer, and so when they find a way around it, you know, little be known to the Spammer, you know, the next day we have a new train filter that has caught. And, so, there's a lot of advantage, we believe, in the collaborative filtering approach.

MR. HUSEMAN: I would just make one point. You know, again, we're not here to talk about the pros and cons of various products, but instead various approaches. And with that, John Levine, I have one question, and then I'll let you have a response as well. Is this too hard for the average user, this type of approach?

MR. LEVINE: Given how successful AOL has been with their report Spam button, probably not. And people are very happy to say -- people are very happy to have a hammer they can use to hit their Spam with. However, I'm worried that Spammers are adapting and collaborative filtering is becoming less effective.

The grandaddy of collaborative filters is a system called Brightmail, where they have Spam-trap mailboxes, mailboxes that are legitimately used for anything but seeded on the web pages and stuff. And from these Spam-trap mailboxes, they get vast amounts of Spam,

all filtering back to Brightmail's headquarters, where they have three shifts of highly trained geeks looking at the stuff coming in and updating filters in realtime that then are shipped out to filtering servers that their customers use.

And it's a great concept, and when Brightmail first came out, it was a killer. It caught all the Spam. But looking now, I happen to have a few mailboxes that are behind Brightmail filtering, and now it catches maybe two-thirds of the Spam, you know, and Brightmail -- and Brightmail is run by very competent people. And, so, I am -- I have some doubt that collaborative filters in the long run can do much better than that.

MR. SARREL: There is one advantage to collaborative filtering, though, which is that if it's not catching all the Spam, it's certainly not creating any false positives.

MR. LEVINE: It's negligible, yeah. The only time you get a false positive is when you report a Spam and then the ISP writes back to you with a response. It happens to quote the Spam that you reported. But that's actually easy to white list.

MR. HUSEMAN: I just have one point of clarification. A false positive, of course, is a message that is labeled as Spam that is, in fact, not Spam. On

these collaborative approaches, though, if it's up to the individual to label something as Spam, you know, as we've been talking about for the past three days, no one can really agree on a definition of Spam, so how can there be no false positives if it's up to the individual to report each message as Spam.

MR. LEVINE: Generally, the number of people that you are accepting reports from is large enough that the only ones that pass the filtering threshold is stuff that everybody agrees is Spam.

MR. HUSEMAN: Now let's talk about some of these sender identification approaches. And, Dan Tynan, what about the challenge response system? Does this work and what are the pros and cons of that?

MR. TYNAN: Well, I tested a challenge response system recently, and I heard back from a couple of people who said why are you challenging my e-mail? Why are you inhibiting my ability to communicate with you? And I said it wasn't me, it was my filter. But they had a valid point, and, you know, that is one major problem with challenged response. Another problem is dealing with automated e-mail. I get a lot of it. I'm on a lot of newsletter lists, and challenged response really doesn't work there. You have to manually add them to your white list. And, you know, it's not infallible.

Until recently, I would have said, you know, the advantage for white list with challenged response is it's 100 percent effective, but I tested one recently and I got some Spam, and they were on my accepted sender list. And I have no idea how they got there. But I'm trying to find out.

MR. HUSEMAN: Matt Sarrel, will senders of messages that receive a challenge, will they respond to those messages, or is that too much work?

MR. SARREL: I think it's too much work. In my experience, having run several of their products that rely on challenged response, there are a few things to consider. One, if the person -- if the sender doesn't quite understand the challenge response method, then they don't really know what's going on. They don't know if it's a legitimate challenge. And, also, it may not even make sense to them, at which point they'll just hit delete. They won't understand that you didn't actually get their original message. And the other thing with a challenged response is that they're not perfect. One of the challenge response products sends you an e-mail, how many kittens are in this picture, and guess what, no matter what you answer, it accepts that as a valid response.

(Laughter).

MR. SARREL: So, there's actually a pretty easy way around that. And, finally, one other thing that concerns me a great deal is that the other day, while I was testing this challenge response, I got an e-mail, I sent a challenge back, I got a response back that included a challenge.

(Laughter).

MR. SARREL: And that wasn't a good system.

(Laughter).

MR. HUSEMAN: John Levine, what is your thoughts on the challenge response?

MR. LEVINE: I don't like them at all. Partly it's that, you know, they're insulting. Somebody's saying I'm much too important to listen to you unless you beg. Partly it's that they tend -- is that they're very difficult to implement without making egregious mistakes. Every time I write to a large mailing list these days, I always get back a couple of challenges from broken challenge systems that don't recognize that it's mail from a mailing list.

I think challenge -- something like challenge response could work, but it would have to be more -- but it would have to be one where the challenge was not sent as e-mail but it was sent by some other scheme that couldn't be misinterpreted as e-mail. And this gets back

more to things more like trusted sender, where you -- where basically the challenge goes back to sort of a separate place that says was this message really from you, but not sent as e-mail. Those -- you know, those could be built on principle, but not many of them really exist yet and they're not widely enough deployed to be widely useful.

MR. HUSEMAN: Talking about trusted sender, Dan Tynan, what are the benefits to consumers and some of the negatives of using a trusted sender program?

MR. TYNAN: Well, trusted sender generally relies on a large number of people using the same system. I think the main drawback would be critical mass in that case.

MR. HUSEMAN: Can you explain that a little bit more?

MR. TYNAN: Well, the system -- for example, there's a system done by Habeas, and I'm willing to bet that Ann Mitchell is here, that inserts copyrightable, trademarkable material into the header of an e-mail message. It actually inserts a poem, a haiku. And people who sign a license agreement to use this can insert the text into the headers of their e-mail messages, and then that's identified as a verified certifiable sender. And people who fake it, people who

are Spammers who put the haiku in, can then be sued for a lot more money than they could be sued under normal law, because they're breaking, you know, copyright law.

And, so, this is a disincentive. And this has already happened. You know, Habeas has already sued people. So, the advantage there is you do have a -- you know, not only a way of identifying good actors, but you also have a means of redressing bad actors. The bad part is you really need everybody using the same system.

MR. HUSEMAN: So, if you were a consumer who used a trusted sender program, and there is currently -- let's say that there's not a current system that has a critical mass of users that you can trust, how is that practical? Can you only -- can you accept mail from trusted senders and no one else? I mean, what are the issues here?

MR. TYNAN: You know, I'm not familiar enough to really give you the details on it. I think one of the presentations later involves trusted sender.

MR. HUSEMAN: Matt, what's your thoughts on the trusted sender technological approach?

MR. SARREL: I'm in agreement with Daniel that it's going to be a critical mass issue. And, also, one thing that I see is how much do you trust the trusted sender? So, is that -- like, is that going to be the

next Spamming technique, how to get around a trusted system, and perhaps Vincent will shed some light on that later.

MR. SCHIAVONE: I'd be happy to.

(Laughter).

MR. HUSEMAN: Now let's take a moment for questions about these various approaches, before we move into our structural changes to e-mail portion of the panel. And, again, as I reminded the panelists, I'd ask the audience members who are asking questions, let's not have your questions be commercials, but let's have them as actual questions and discussions about these approaches.

Does anyone have any questions about some of these various approaches currently? Yes, way in the back over here.

MR. FERMANSKY: McLean Fermansky, I-space Research Labs. Gentlemen, I'm afraid that your technological solutions don't solve one problem that still stands. It's been alluded to a few times, mentioned a couple of times, and that is cost-shifting. I'd like to use the figures from Mr. Lewis from Nortel. If he were my ISP, he would be running a machine and hiring personnel to carry 400 percent more traffic than he would have to otherwise, if there weren't Spam.

Now, Chris is a nice guy, but he's a businessman, as my ISP, and he's going to be charging me for that. Likewise, his upstream provider has to carry that bandwidth, charges him, he charges me. Gentlemen, your solutions only handle Spam that has arrived. I may have a 100 percent effective filter, but it only works on the Spam that's arrived and it doesn't do anything to stop that traffic, to block that bandwidth.

MR. HUSEMAN: John Levine, what's your response to that?

MR. LEVINE: To a large extent, you're right. In the source filtering approaches tend to knock away -- knock down much of the cost by preventing you from receiving the mail, but, I mean, all these filtering techniques fit into the current -- the current design of mail, which as we -- as somebody commented yesterday, the fundamental model is one of the sender freeloading on the recipient. And to fix the cost-shifting requires some fairly fundamental -- deeper changes to the structure of e-mail than we had discussed so far.

And I think we can look at them, but I think it's not -- I don't think it's a very promising approach, just because I think that that deep a change to the structure of e-mail, both is something that we don't know how to do and something that even if we did, it took us

10 years for people to move from random proprietary mail systems to SMTP, and I'm afraid it would take 10 years to move from SMTP to anything else.

MR. HUSEMAN: Vince Schiavone from ePrivacy Group.

MR. SCHIAVONE: Well, a couple of things. There is technology available that goes in front of the receiving servers that can analyze traffic paths and, in fact, reverse the economics by slowing the ability to deliver. Right now the economics of Spam are delivery over time. And much of the Spam-fighting -- the Spamming technology moves on if the connection and receipt is too slow on the uptake. So, by analyzing it, you could call it a pre-filter or a squelching technology. You can then slow up the Spam and inhibit their ability to deliver as much and their profit and reduce the costs on the enterprise or the ISP.

MR. HUSEMAN: Paul Judge?

DR. JUDGE: The question was about cost-shifting, and I think the person asking the question was alluding to some of the technologies that add a monetary cost to sending e-mail, but I believe there's other ways to shift the cost and really aim at the profit of the Spammers without necessarily introducing a cost for e-mails. I think that a number of solutions that we're

working on, even detection systems, focus on shifting the cost, at least reducing the profit of Spammers.

If you look at Spamming, it comes down to a business, and it's about making a profit and what that entails is the amount of money that the Spammers make, minus the amount of money that it costs them to send the Spam, and the amount of money that they make is affected by a couple of parameters. And one of those is the number of Spam messages that are actually received by end-users and the response rate.

So, the number of messages that are received, we have the ability to affect that by the effectiveness of our Spam filters and also the deployment percentage of Spam filters. The response rate, we have the ability to affect that with best practices and user education. And then some of the other costs that we're able to introduce into the system are kind of the cost of litigation and the legislation and going after the Spammers in that manner.

MR. HUSEMAN: With this panel, we're really focusing on kind of the technological issues in regard to cost-shifting. Is there a technological way to -- what would you recommend?

DR. JUDGE: So, what I just mentioned was that there's two variables that we can affect with technology,

and it's really the number of messages received, and that affects the profit that they make. The number of messages sent affects the amount of money that it costs to send out that Spam flood, and the number sent minus the number received is affected by really the effectiveness of your Spam filters and the deployment or percentage of the Spam filters. So, just saying that even without introducing a system that charges for e-mail, we have the ability to affect the profits of Spammers.

MR. HUSEMAN: Steve Atkins from Word to the Wise and SamSpade, what is your thoughts on technological solutions to cost-shifting?

MR. ATKINS: Not so much to cost-shifting specifically, but in regards to rolling out new protocols, yeah, it took many, many years to go from proprietary e-mail to SMTP, but compare that with instant messaging. If the consumer, the user of the new protocol, sees the advantages of it as being huge, then you can roll out new protocols very quickly.

Currently, SMTP is being used for an awful lot of things, perfectly legitimate things and some Spam as well, but it's just really not very well suited to. If some of the traffic that currently is going over SMTP were rolled off onto a more appropriate protocol and it

was backed by AOL, Microsoft, Earthlink, Yahoo, Hotmail, then I could see new protocols being rolled out in months rather than years.

MR. HUSEMAN: We're going to get to that in just a little bit about some of the protocol changes. Matt Sarrel, what about the current technological approaches that we have and reversing the cost-shifting in Spam?

MR. SARREL: We had looked at a number of gateway devices, which Vincent mentioned, and these function similar to -- if you think about a firewall, at the edge of your network, in front of your mail server or in front of the ISP's mail server, and so what they do is not only do they filter the content of e-mails and they can also utilize white lists and blacklists, but there can also be the reverse DNS queries to make sure that the sender is legitimate. And they also look at SMTP traffic that is abnormal, such as someone trying to harvest e-mail addresses from your system using random characters. That's not a typical behavior when trying to send a message.

So, if you deploy a gateway device, then that keeps the e-mail from getting onto your systems and using up your resources, which does not entirely address the issue of cost-shifting. However, I think part of the

problem is that when we all go out and develop our anti-Spam products, we want to give people something that they see. So, if you -- you know, there's a big differences between a product that you install on your desktop and the next day you see it stopped two-thirds of your Spam and a product that gets deployed at an ISP and it takes a year or two and then we stop getting Spam. I think that the whole product development cycle is part of the issues.

MR. HUSEMAN: I have one quick question for some of the panelists, and then we're going to move on to some of the specific technological approaches that are being proposed currently. Let me ask John Levine, let's say your grandmother, to use a grandma example again, is setting up an e-mail account. What approach would you advise her to use?

MR. LEVINE: I'm thinking about my dear stepmother, who's a very smart lady, but her expertise is not in computing. And at this point, I would tell her to use an ISP who's got built-in Spam filtering that she doesn't have to mess with, because as someone else commented, the person running the mail server can do a lot better job of filtering than the end-user, just because it has a lot more data at its -- to use, and it's got a lot more compute power to throw at it. And at this

point, you know, there's not much more useful that I can tell her.

MR. HUSEMAN: Now, Dan Tynan, let's make the example now your teenage son or daughter.

MR. TYNAN: Okay.

MR. HUSEMAN: What approach would you tell them to use?

MR. TYNAN: I think I'd just lock them in their room away from the computer.

(Laughter).

MR. TYNAN: I'm hoping to do that anyway. They'd be more sophisticated, they'd be much more savvy. So, there won't be the technological barriers there are for John Levine's dear stepmother. But they will still be faced with a problem that the off-the-shelf Spam filters and the built-in Spam filters in things like AOL and Yahoo and MSN just don't -- aren't 100 percent effective.

So, my point of view on this is the whole purpose of Spam filtering software is to kind of turn back the clock five or six years, to the point where when we used to get e-mail and not Spam, at least not very much of it. And, so, it should be as close to mimicking that as possible, which means I would recommend something that goes right into the e-mail program you like to use,

filters it automatically and requires minimal interaction.

Unfortunately, most Spam filters require some interaction, because you have to look for false positives, but that's the approach I would go to. I would say okay, look at your e-mail program, your client, whether it's Outlook or Outlook Express or Eudora, find one that filters Spam inside that program with one or two clicks and go for that one.

MR. HUSEMAN: Matt Sarrel, let me ask you this question. What approach would you recommend for yourself or approach do you think works the best, or approaches?

MR. SARREL: Well, I'll tell you what I do. It's sort of along the lines of the disposable e-mail address model. And this, by the way, is just what I do personally. For work, we have this situation where I need -- I basically need to receive Spam, because some of it is a product announcement. Whether there's value in that or not, I won't comment.

So, what I -- I have three e-mail addresses. One is sacred. I don't give that out to anyone except for my friends. And you could sort of think of that as the white list model. And I don't -- I actually have not yet gotten any Spam there. The next account I have I use when you have to sign up for something, like -- but it's

something that you might want, like a newsletter or a shipment confirmation, an order confirmation, something like that. I get more and more Spam in there. And the third one is an address that I have where this is, you know, go ahead, Spam it, I check this once every two months just to keep it active, and it's where they force me to sign up for something, just to check a website, or if, you know, someone's giving something away and they need an address.

So, it's three levels of sort of what you would think of along the lines of like trusted sender or white lists. And admittedly, that's complicated. Like I wouldn't expect my mother or John's stepmother to be able to handle the three-address system.

MR. HUSEMAN: Let's change topics a little bit. Ryan Hamlin from Microsoft, you're the manager of the Anti-Spam Technology and Strategy Group there. As we know, AOL, Microsoft and Yahoo just came out with several proposals, and the proposal had four parts. I want to ask you about some of the specifics about that. The first one -- your first approach was protecting consumers from receiving Spam, and you talked about using the domain name system to better identify the location from which e-mail is originating. What does that mean and what is your proposal?

MR. HAMLIN: I'll speak as best as I can on behalf of the other companies, but defiantly should follow up with AOL and Yahoo, because I don't want to misrepresent them. So, from a Microsoft standpoint and what we kind of got out of this alliance is that around the best practices for protecting our consumers, we thought DNS made a lot of sense, because it's global.

MR. HUSEMAN: And DNS is?

MR. HAMLIN: DNS, domain name servers -- server. So, it's global, it's distributed, it's well understood today and it really is the means obviously for the identification today.

MR. HUSEMAN: And, so, the DNS is where the internet protocol address matches up with the domain name?

MR. HAMLIN: Give it a domain name and get the -- exactly, get the IP address back. So, we felt like we want to leverage an existing technology that's well known and well understood and distributed. And there's multiple approaches to that. We talked about RDNS. I know John talked about reverse DNS as one way of potentially doing that. I mean, with this identity crisis, domain spoofing is one of the biggest issues that we need to really focus on in the short term. We believe that solving a lot of the identity issues will help -- is

a big step forward on reducing Spam.

MR. HUSEMAN: So, how does this proposal do that?

MR. HAMLIN: So, what we've said is that we want to leverage DNS and that we need to get in the room with others, because certainly Microsoft, AOL and Yahoo don't want to dictate to the industry exactly what to do. We want to definitely open this up to other independent parties and the consumer groups and the marketing organizations to get some feedback to us, but the idea is either via reverse DNS, to make sure everyone has a reverse DNS entry, so to John's point, when you do a reverse DNS, there actually is an entry there and you can associate the IP to the domain. Another approach that -- and this is a Microsoft approach that we've just kind of thrown on the table -- is to put the IP addresses in the text field in DNS, again, the idea being --

MR. HUSEMAN: What does that mean?

MR. HAMLIN: So, much like the example I think on the first day, where they spoofed -- I think it was the gal from Yahoo that spoofed basically a mail coming in to the FTC, and basically pretended to be somebody from FTC and the mail coming in, and even though she was logged -- actually, it was an AOL person -- even though she was logged into the AOL domain and had an AOL IP, she

was spoofing that she was coming actually from ftc.org.

So, by having this solution, what the ISP would do or the in-bound receiver of that mail would do, would do a lookup and say this person claims to be from Hotmail, this person claims to be from ftc.gov, what is the associated outbound IP addresses that they send mail from, does it match? Oh, it doesn't, so in that case, it wouldn't have matched, because that IP would have came back as an AOL IP, and it would have been matched to the wrong domain, an ftc.gov domain. And, so, instantly you would have known that that was Spam and you could junk that mail.

MR. HUSEMAN: So, if one was sending e-mail from an AOL domain name, yet it was actually coming from a Hotmail IP address, then you would be able to tell that?

MR. HAMLIN: Correct.

MR. HUSEMAN: And prevent that form of spoofing? But this proposal would not prevent someone -- that has an actual Hotmail account in using a Hotmail IP address from spoofing one of the other millions of Hotmail users? I mean, is that right?

MR. HAMLIN: Agree. I mean, this is going to be, you know, a multi-step approach. We believe that this is a great first step forward. We also believe that

a lot of the terms of use and the policies that are in place at the ISPs, by having this step forward, it will give the ability to really screen that out. And if within each of the ISPs, I can just speak for Hotmail today, one of the things we've done is we've locked down, for example, you can only send 100 mails a day. So there are certain things within the ISP, then, you can take the next step once you've got the identity crisis kind of in order.

MR. HUSEMAN: Steve Atkins, what -- is this effective? Will this do anything for the average consumer's inbox?

MR. ATKINS: Well, it will break e-mail. This is basically a variant on designated sender, which has been discussed fairly widely recently on a number of mailing lists where people are discussing this sort of approach. And while it looks tempting on the surface, there are some fundamental bits of e-mail that can break, like e-mail forwarding, e-mail exploders, mailing lists, if it's not implemented absolutely perfectly.

MR. HUSEMAN: And what do you mean by those things, e-mail forwarding?

MR. ATKINS: Well, if you sign up for -- if you have an e-mail account and you don't want to actually receive your e-mail there, you want to forward it on to

your new ISP, you can tell your old ISP to forward the mail on, depending on how that is implemented, it can look to the receiving new ISP like the incoming mail is Spam. At that point, if the new ISP is using a designated sender type protocol, it could mistakenly discard all the mail that was forwarded from your old ISP as Spam.

MR. HUSEMAN: Ryan Hamlin, what's your response to that?

MR. HAMLIN: So, agree that the way that you set it up, we need to have explicit directions. There's actually, you know, plenty of ways around that, both RDNS and the idea of embedding IPs in a text field. One solution would be embed additional IPs. You don't just put, you know, your mail server IP. If you use an ISP to send your mail for routing, you would have their IP's address in there, as well. So, you would basically allow for in that text field multiple IPs to get around the scenario that Steve described. It's a very real scenario. You would just need to be careful and have explicit instructions and well known in the industry of how to implement that.

MR. HUSEMAN: Steve Atkins, do you think that consumers will do this or will be able to do this?

MR. ATKINS: This isn't something consumers

would do. This is something ISPs would either choose to do or not choose to do. It's an interesting concept and a lot of people are interested in playing with it. How much of the network it will break when it's deployed, we're probably not going to find out until somebody deploys it and sees.

MR. HUSEMAN: John Levine, what are your thoughts on this proposal?

MR. LEVINE: I'm actually with Steve here, because I've -- this is -- in my taxonomy, this is what I referred to as designated sender, list the valid places, list the approved places that mail from certain domains can come from. It's certainly a way to keep down on spoofing. But, I mean, certainly on my own network I have a lot of indirect web hosting customers, and mail sent to webmaster@, you know, whoever it is, is then remailed off to wherever their actual ISP account is, and all of that mail will be broken by a straightforwardly implemented designated sender scheme.

I mean, I think there are ways around it, but for a lot of these changes, you really have to weigh off -- you have to balance to what extent will this break the way that mail works today and is the cost of that breakage worth whatever benefit it's going to provide. And in the case of designated sender, I think the jury is

still definitely out. I couldn't tell you either way.

MR. HUSEMAN: Ryan Hamlin, what does Microsoft see as the implementation and the timing of this change?

MR. HAMLIN: That kind of approach? So, like I said, I mean, we want to make sure that -- there's a lot of really smart people, and we've had a lot of great opinions and debate about this. I think it's very important, events like this are great because it will force us to move in a quick manner. And I agree with Steve, we need to do some of this trial and error to get it done. So, our plan is, again, to quickly open this up to others. Again, we don't want to just dictate it, Microsoft, or Yahoo or AOL, and get some additional feedback and opinion from others, but then we look for a short time frame to try it out, because we think that's an important next step.

MR. HUSEMAN: Paul Judge from the Anti-Spam Research Working Group, which we will talk about in a moment, but what are your thoughts on this particular proposal?

DR. JUDGE: So, within the Anti-Spam Research Group, a number of things we're looking at. One of them, of course, is authentication, and we do have a very similar proposal that has been put on the table and designated sender, we refer to it as reverse MX lookup.

There's reverse DNS. I think what he just described refers to a reverse MX lookup. And I think that it's something that can be deployed incrementally.

It doesn't require that one day everyone turns it on and we begin to drop the rest of the e-mail and break e-mail. If a domain decides to turn it on, then they've prevented forgery for their domain and they're protected. For persons that have not turned it on, then their e-mail still flows but they are not able to stop people from forging messages from their domain. So, I think it's something useful and can be deployed incrementally.

MR. HUSEMAN: Ryan Hamlin from Microsoft, the second part of yours and AOL's and Yahoo's proposal was eliminating the ability to create fraudulent e-mail accounts in bulk. Is that the limitation of sending out 100 messages per day, or is this a different proposal?

MR. HAMLIN: Yeah, so to the earlier question about raising the cost barrier, we think it's really important to raise the cost barrier for Spammers to get accounts. So, when there is an opportunity for a free account or a nearly free account, meaning we don't get a full credit card and we're charging, you know, a full-access fee, we want to put a barrier in place so that they can't automatically -- Spammer can't automatically

generate mass accounts in bulk.

So, a few months ago, you could go out to Hotmail and it was free accounts and you could have automation to create thousands of accounts at a time. We've since put something we call HIP, or human interactive proof, in there, in the sign-up, so that when you sign up, it gives basically a set of letter combinations that are not readable by the machine, that requires a human to put in exactly what that is, and then respond, and the create is actually -- the account is actually created.

So, we've seen a drastic account of the bulk creation, once we put something like that in, so it's saying where there is a low cost to barrier for mass bulk accounts, we need to put a mechanism in place to stop that. That's just one approach that we put in as an example at Hotmail.

MR. HUSEMAN: Steve Atkins, what do you think of that approach? Is that effective?

MR. ATKINS: Yeah, there's been a number of cases for, oh, years back, where free web mail providers have been abused by bots in this way, and the approach Microsoft is suggesting is a well-proved, good one.

MR. HUSEMAN: John Levine, any thoughts?

MR. LEVINE: I agree that it's a well-proved

scheme, and if I may tweak you a little, Microsoft was a little behind the curve on this one.

(Laughter).

MR. LEVINE: Honestly, I think that something that's outside the purview of this panel, but what we really need is a credit bureau for ISPs, so that when you have someone who's been kicked off one ISP, it's harder for him to sign up on another one, you know, which is, you know, a completely non-technical thing, you know, it's what credit bureaus do. And the world desperately needs one specifically to meet the needs of ISPs.

MR. HUSEMAN: Microsoft, do you support the creation of such a bureau of information sharing between ISPs of Spammers who have been kicked off?

MR. HAMLIN: Yeah, in fact, I think the next bullet point in the press release talks specifically about that, about sharing that information. So, you know, the great thing that I thought about the announcement was, although, you know, Microsoft, AOL and Yahoo are fierce competitors and will continue to be fierce competitors, we do have one foe, and it's the Spammer.

And, so, you know, over the months of us talking, we realized that there are some best practices we can share, so things like that, where we've identified

a Spammer on our network, there's no reason why we shouldn't be sharing that with the other ISPs to take advantage of that, because it is solvable by an industry, because what's happening is the Spammer just hops to the next network.

MR. HUSEMAN: So, what type of information will you share?

MR. HAMLIN: So, there's a lot of -- there's kind of two different ways. One is sharing where we identify, obviously, harvest attacks or fraudulent account creation via an IP. So, we potentially will be discussing ways amongst the ISPs to share that information. Again, we're not going to -- because of the issues around blacklists, so you have to be very careful there when you start sharing IPs.

The other area that we talked about is in the area of enforcement, where we start to share electronic evidence, and that kind of goes into the fourth point, but it's where the ISPs work together to provide an electronic record, and so instead of just a Microsoft going after a particular Spammer, it's really the industry of ISPs going after these folks and providing up information across all ISPs.

MR. HUSEMAN: What type of electronic information does the proposal anticipate you sharing?

MR. HAMLIN: So, you've got to be aware, obviously, of the privacy information, but the idea would be we would start to log some of the activities. So, as there would be suspicious or fraudulent type behavior, we could notify the ISP community and others that have witnessed that same type of behavior, maybe associated with a given IP could start to track some of that information and logging. It doesn't mean black list them, it just means track that, so if it does turn out to be something of fraudulent behavior, we have that record.

MR. HUSEMAN: And when will that -- this take place? What is your time table for implementation of this?

MR. HAMLIN: So, I'm going to sound a little bit of a broken record, but really what we want to do is get the feedback from others, because we know, again, the three of us alone can't solve this thing, so we need to understand the technical implications across the board for small ISPs to do this, for medium-sized and the large ISPs.

MR. HUSEMAN: And, so, when are you going to get the feedback from others?

(Laughter).

MR. HAMLIN: So, it's a great -- so the plan is to absolutely in the very near short-term --

MR. HUSEMAN: Such as?

(Laughter).

MR. HAMLIN: I should have known with a lawyer.

(Laughter).

MR. HAMLIN: So, our plan is within the next couple of weeks, we will have another discussion, the initial ISPs that I talked, and then within a very short time after that, let's say, you know, 30, 60 days, we'll get together as an -- and invite the broader community to participate. So, this is something that will get done in the next couple of months, not something that's going to get done in 12 months from now.

MR. HUSEMAN: And will this -- these discussions and feedback, will that also include the credit bureau/Spamming bureau sharing of information? About people who have been kicked off? Will that be part of this discussion that you're talking about?

MR. HAMLIN: Oh, yeah, all these four pillars that we kind of laid out in the press release, those will all be discussed at that type of a forum. And we will -- you know, we'll take a look at identity crisis, and we'll propose the idea that we talked about already. We'll look at other ideas, too, though, you know, that Paul is looking at, and others in the industry.

But the key is, and I said it before, we have

to show movement. It's an incremental process, but we've got to show movement. And this is a great forum over the last, you know, couple of days, to just do that, get in a lot of really good feedback. We now are ready in a position to move.

MR. HUSEMAN: Steve Atkins, what would you say to Microsoft about this?

MR. ATKINS: It's a very good idea.

(Laughter).

MR. HUSEMAN: Paul Judge, what would you say to Microsoft about this?

DR. JUDGE: I will be talking to Ryan further about this. We had some initial conversations. Also, I'm going to talk to another group that represents a different set of constituents in this ecosystem, and they have a detailed proposal coming out in a few weeks that looks at just that, a reputation system. I think it's really a good move from black lists, which used to give us a binary decision, to something like a reputation system that gives us more detailed information about a sender, about the bulk of mail that they send, about the number of complaints that they have, and then we're able to make more granular decisions about that sender.

MR. HUSEMAN: David Berlind, I want to move to you now. You are the founder of something called

JamSpam. This is a consortium that you put together of various industry and various other representative groups to try to come up with a solution. Can you briefly tell us about this group and what are your specific proposals and the time frame.

MR. BERLIND: Thanks, Brian. First, I think that Commissioner Swindle gave me the ultimate lob that anybody could ever dream of this morning when he said that it's up to everybody in this room to work together to arrive at a solution, and there is no one particular solution, so whether it's a technological solution or a legislative solution, none of them will work well if they're not harmonized to work together. It's sort of like getting the different federal agencies to work together to prevent terrorism, if they don't work together, the dragnet will never be sufficiently closed to keep terrorists from slipping through.

There are six distinct communities that must work together in order for any solution, any one particular solution, to work in concert with the others. One of those is the ISPs and in-box providers; the other one is the e-mail client and server providers; a third is the e-mail security and management providers. These are people who make products that run in parallel to the e-mail client and servers.

Then there are the high-volume e-mailers, the ones who are often accused of Spamming and maybe are not Spammers. I'm not here to pass judgment. Then there's a group of organizations that I refer to as the non-commercial and non-profit privacy and anti-Spam advocacy groups. And then finally the end-users.

All of these proposals, if each of these communities goes off and works on their solutions on their own, without consulting with the other communities, it runs a risk of creating a solution that will undermine the solution another community is working on. I'd like to just say that to the extent that Microsoft, AOL and Yahoo are soliciting input from the rest of these communities, JamSpam is to this day the only forum and it's the only one where all of those communities have so far gathered to discuss the problem. And that's what JamSpam is about. It's about all of these communities figuring out a way to work together.

And just by a show of hands, so everybody's really clear on the type of participation we're talking about, we have leaders from every one of these sectors, by the way, including AOL, Yahoo, Earthlink, Microsoft. In fact, I saw them all exchanging cards for the first time at the JamSpam meeting. I'd like to think that that's how this collaboration came to be.

But could everybody in the room who is some way related to JamSpam, attended a meeting or something like that, raise their hands.

So, there's quite a few people in this room and they represent all the different -- Paul Judge, you didn't raise your hand.

(Laughter).

MR. BERLIND: Vince, did you raise your hand?

MR. HUSEMAN: Okay, David Berlind, so what is the specific outcome of JamSpam? What is your goal?

MR. BERLIND: Well, the goal is that knowing full well that something like the IETF has to produce a protocol or enhance the protocol, as Steve said, and I think I absolutely agree with that, we need a hardening of the protocols. The hardening of those protocols shouldn't be done without consultation from each of these communities, so that we understand what the impact of any hardening is.

To the extent that legislation is being proposed, legislation shouldn't take place without consulting with the technical community to see whether it makes sense. I mean, it makes no sense, for example, to enforce laws in different states if you have no -- if the e-mail technology is blind to the geographic location of the sender and the recipient.

MR. HUSEMAN: Let me interrupt for a minute. Does JamSpam hope to introduce a specific technical protocol or technical solution as a result of group discussions?

MR. BERLIND: I think that early that was the goal of JamSpam, was to create a new protocol. When we suddenly realized that there are existing intellectual property organizations already in place that are capable of doing that. The goal switched to being one that develops a 360-degree view of the complete problem that all of these communities then can work off of as a unified front in harmony with each other.

Right now, each of the communities is working off of roughly a 270-degree view of the problem. And if they only address those 270-degree views, then what ends up happening is some part of the problem is ignored and two solutions from different communities end up stepping on each other. Blacklists is a perfect example.

MR. HUSEMAN: Well, what is your time frame for the JamSpam for whatever proposals or discussions?

MR. BERLIND: Well, so far, we've had two meetings. The first was in February, and the second was in March. And last I heard, America Online volunteered to host the third of these meetings. The second meeting produced the 360-degree view. The third meeting is to,

technically speaking, to produce sort of a charter for the organization, how it will work with organizations like the IETF, government bodies, a variety of different organizations to move the ball forward in a way that again all the parts are moving in harmony with each other, not going off in separate directions doing their own thing.

MR. HUSEMAN: So, you don't have a specific time frame for any end-product or resolution of this, or is this more an ongoing discussion?

MR. BERLIND: I think it's an ongoing discussion. I think that the number one priority, though, just to comment on what some of the other panelists have said is that one of the reasons a lot of different things don't work is that there's no critical mass. The only thing that's going to achieve critical mass is a standard that's in place that's complied with by every system that's out there.

And, so, the number one priority for JamSpam is to make sure that such a standard is created and put in place as quickly as possible.

MR. HUSEMAN: And, Paul Judge, you are with the Internet Research Task Force, Anti-Spam Research Working Group. Did I get that right? That's a lot of words.

DR. JUDGE: Correct, yes.

MR. HUSEMAN: Briefly, what is the Internet Research Task Force and what is your working group?

DR. JUDGE: The Internet Research Task Force is the -- well, it's just an organization of the Internet Engineering Task Force, the IETF, that standardizes many protocols, the body that standardized SMTP and HTTP and so on. The Research Task Force has historically consisted of just a small number of groups focused on problems that are important to the future of the internet.

And we formed the Anti-Spam Research Group to focus on just that, the problem of unwanted messages and from the viewpoint of a networking problem and seeing how it's affecting local networks and internet and so forth. When we chartered the group a few months ago, we charted it realizing that the definition of Spam is really inconsistent and not clear, so we generalized the problem into one of constant base communications, meaning that an individual or an organization should be able to define either consent or lack of consent from certain types of communication. So, from there, our goal is to first understand the problem, collectively propose solutions and then evaluate those solutions.

MR. HUSEMAN: So, what authority or incentive is there with the IRTF, for whatever proposals you come

up with for the internet community at large to adopt.

DR. JUDGE: So, I believe, in general we're dealing with the Spam problem, it's not hard to motivate the problem. So, I don't believe that we need to provide much incentive for people to do the work. The research group really provides a forum for people to come together to collaborate on a common ground. I think previously that there's been many individuals interested in the problem, and we've been in different corners of the world working on the problem. And we began to have meetings like this and on the research group meeting, only in January of this year that this group of people began to come in the same room. So, through the research group, our goal is to bring these people together and have some collaboration on the problem.

MR. HUSEMAN: So, your group will possibly come up with new protocols?

DR. JUDGE: So, a number of things, as I mentioned. It's really three phases. One is to understand the problem. The second is to propose and collect proposals for solutions. And then to evaluate those proposals. And as far as understanding the problem, I believe that we know a lot about the size and the growth of Spam, but there's many characteristics of the problem that we don't understand as a community.

Traditionally, any problems in networking and security, there's a lot of effort to characterize that problem and to understand and allow trace data to be established so that we can study exactly where we need to focus. And that hasn't been done traditionally. We've taken more ad hoc approaches to the Spam problem. So, we're really trying to take a more systematic or research-oriented approach to it.

And the second piece, as I mentioned, was either proposing solutions or first of all collecting the solutions that have already been proposed. So, one thing that we did that was very important was to establish a complete taxonomy of all the solutions that have been proposed over the years and to begin to understand how those interrelate and how they can be put together to leverage the benefits of each other.

And the third piece, as I mentioned, was evaluation. And I think over the years, that solutions have been proposed and persons have gone out and deployed those solutions, and it wasn't a lot of thought put into the evaluation, not only of the effectiveness and accuracy but also the burden of introducing this and how robust the solution is to countermeasures, and that's how we got ourselves into the cat-and-mouse game that we're into.

So, as we think through the solutions now, we're able to make better decisions, and objective ones, about the solutions that we propose and move forward with.

MR. HUSEMAN: What is your time frame for your Research Working Group?

DR. JUDGE: So, the group was chartered a few months ago. We had the first physical meeting in San Francisco in March. We had about 250 participants there. Most of the work is done through interactions on the mailing list and off-line. And there's a number of work items that have been identified and we're currently working on. And there's a range of things, though, everything from the taxonomy to really working on measurement and analysis work.

And there's a lot of collaboration between different companies, ISPs, also different interest groups and whatnot. For example, at the first meeting, as we talked about the collaboration of the different constituents, we had representatives from each of those organizations, and many of the persons I assume that are in this room, were working on different projects. So, I can get into the details of each one of these, but things are ongoing as we speak.

MR. HUSEMAN: So, when do you see the process

being completed?

DR. JUDGE: I don't know, when have we solved a problem? Is it when --

MR. HUSEMAN: Are you talking about months, are you talking about years from now?

DR. JUDGE: I think that -- you said the process being complete, as far as the work of the research group?

MR. HUSEMAN: Yes.

DR. JUDGE: Something that's -- there's short-term deliverables as well as medium to long-term deliverables. And some of the short-term ones are the analysis and the taxonomy work. And then there's some short-term to medium-term actual solutions that we can roll out, mainly the identification systems, things such as reverse MX and the reputation systems that we talk about, introducing authentication and accountability into the system are short to medium-term, so you know, six to 12 months we can begin to roll some of these out incremental.

And then from there, there are more long-term things that we want to do, as we chartered it with this view of a consent-based communications framework, that's something that's definitely more long-term, allowing us to have granular definitions of different types of

messages and be able to enforce that policy. So, you know, to get to a perfect system, it's a few years, but to significantly affect the problem, it's more short-term than that.

MR. HUSEMAN: John Levine, what are your thoughts on the IRTF's working group efforts? Are you involved in this group, by the way?

MR. LEVINE: I stopped reading their mailing list a couple of months ago, so I don't really know what they're doing now.

MR. HUSEMAN: And is there a reason you stopped reading their mailing list?

MR. LEVINE: I have to say -- I talked to Paul a little bit a couple of nights ago, which is I didn't get the impression that the people in this -- at least on the mailing list had done their homework very well. I mean, I saw a lot of suggestions coming up and saying, you know, sort of suggestions that looked awfully familiar and that if -- I mean, I think a taxonomy is great, but I think also a taxonomy of how approaches have succeeded and failed would be -- is really important. I didn't see much appreciation at that point for all the work that had been done and the subtlety of some of the problems that people had run into.

MR. HUSEMAN: Paul Judge, your response?

DR. JUDGE: As he said, he stopped reading the mailing list a few months ago. I don't believe that he's looked into the details of the taxonomy or probably would have had some input into the one that was presented. But the point is that we have a research group and we announce that we're working on Spam, and there's many people across the world that are very sensitive and very emotional about this problem, everyone ranging from people that sit here that work on it day in and day out for the last couple of years to people that are end-users that want to affect the problem and believe that they have a bright idea.

So, as this open research group, as we're currently chartered, we must deal with that entire range of persons, so, there is, you know, some noise on the mailing list that is not the most insightful contributions, but there are many work items that are defined and are being worked on in the mailing list. So, persons that are paying attention to the mailing list can understand and appreciate that.

MR. HUSEMAN: Steve Atkins, will such an approach be effective with so many different users involved?

MR. ATKINS: Such an approach as the ASRG mailing list or -- I'm unclear?

MR. HUSEMAN: As the Anti-Spam Research Working Group, can this approach or such an approach like that be effective with a solution?

MR. ATKINS: I haven't stopped reading the mailing list, but apart from that, I would agree completely with John.

MR. HUSEMAN: And why is that?

MR. ATKINS: The amount of traffic on the mailing list was very high. Those people who actually work in the industry and understand the issues and have looked at the approaches three, four years ago that the ASRG is revisiting or reinventing now, mostly left in the first three or four weeks, because the amount of signal was low and the amount of noise was high.

MR. HUSEMAN: Paul Judge, what is your response, if you have anything in addition to add, besides what you already said about this issue?

DR. JUDGE: Well, so this is in the first three or four weeks when we really dealt with many newcomers to the area of Spam. This was not the persons that are sitting on this panel or many people in the room, but people that really didn't know much about the problem and came on to the research group looking for answers. And, so, there was a significant amount of noise; however, the research group isn't an entity or a body that exists by

itself. It's really a group of individuals, and it's about individual contribution, and it provides a place for people to come together and work on the problem.

MR. HUSEMAN: So, do you have any specific proposals, or is that later on in your phase? And do you have any specific things about what types of solutions such as this will work, either be it protocol changes or advanced filtering or et cetera?

DR. JUDGE: As I mentioned, there are a range of things we looked at, first of all, the things that have been proposed already, to sort of understand the solutions base and to realize that we've almost completed filling the solutions base, but as far as different proposals, it's individual contribution, and if you look back at the first meeting we had, there's been two major approaches submitted or published this week. One was by ePrivacy Group; and one was by NAI and their Lumos system. And both of those proposals were presented at the first Anti-Spam Research Group meeting. A few other proposals and systems we see information about on the table out there were presented as part of the Anti-Spam Research Group. So, I believe that, you know, a number of things have been funneled through there.

MR. HUSEMAN: So, your position is that this is causing or helping with these proposals to being

introduced, is that correct?

DR. JUDGE: Yes.

MR. HUSEMAN: Okay. Let's talk about one of the proposals that was mentioned. Vince Schiavone briefly is going to talk about what he sees as a structural solution or protocol change to e-mail and describe that.

MR. SCHIAVONE: Having developed the trusted sender program and deploying it last year, we agree very much that there is a critical mass issue and it requires support. We are at some chicken-and-egg situations as far as e-mail goes. One of our large clients challenged us that for anything to pick up critical mass, it really needed to be an open standard that was free and available to all and involved many, many people.

What we heard here today so far is that we've been putting a lot of band-aids on something and we're losing. I mean, all these technologies are getting better and better and better, yet Spam is increasing geometrically in my e-mail box and in the filters before it gets to me. What Commissioner Swindle said this morning is we need to give the ISPs and the consumers a way to decide who and what they want to receive. Well, the who and what is the problem. Foundationally and fundamentally, there is no trust in e-mail. It was never

meant to contain trust, and I don't know who's sending me e-mail.

What I'm receiving, there's no standard way for NAI members to tell me I'm receiving a statement, so my filter people don't inadvertently block it. So, what we've done is proposed here today an open standard where we are willing to contribute our technology and hope others will stand up to contribute theirs, to try to get to the point, using today's existing standards to seriously separate the good e-mail from the bad e-mail. And I'll go through it very quickly, or Brian will kick me off, he said.

(Laughter).

MR. SCHIAVONE: And at 4:00 in the afternoon, that's very sensitive.

What we've learned in the last few years is how not to fix e-mail. Technology can only enforce policy; it can't create it. It can't tell who it is. Policy that's not aligned with technology won't work either, because it can exclude a lot of different people. An important thing that you'll hear us say is the ISPs adopting standards or not adopting standards is the issue that will change how Spam occurs, because so many -- so much of the e-mail goes through them.

How to fix ISPs, we feel, is to use the ISPs

and the laws to encourage both a carrot and a stick approach. The ISPs can block things, okay? But they can also encourage, not give a free pass, but to weigh positive features that people step up to. The laws can create penalties, but they can also create safe harbors for people who choose to do things that encourages good behavior.

Our standard that we're proposing is a framework to provide trusted identity. The commerce on the web today is based on the DNS system with digital certificates layered on top of it, because DNS is not secure. We don't know who's sending. There's spoofing because there is no security, so we have to add it. We need to know with a secure, fast and lightweight method who is actually sending us e-mail, making trusted assertions. We need to know who the sender is, and we should have the ability for them to communicate to us the content of the individual e-mail, and many people in this group, although they may not agree what the permission should be, might think it would be useful that the permission be communicated with the e-mail. We need to create a framework for creating a federation of trusted e-mail programs. JamSpam was a great way to get everybody together, and it's only through cooperation and harnessing all the energy in this room that we get there.

Our plan calls for a small oversight board, very representative of the 360-degree view, okay? Oops, I'm on timing. Did you add the timing to this, Brian?

We believe there needs to be very minimum standards that do not disenfranchise either anonymous individual e-mail, which is very important to the internet, as well as small businesses who should not have to bear high costs. And that should include a basic identity, near zero costs, but create a standard language for stating it and communicating.

We also suggest a standard language for stating assertions, but at this level, it should be optional. It's very sensitive, excuse me. Is it unsolicited e-mail? Is it permission-based? We're not advocating labeling in the subject line. Mail moves very quickly and in large volumes, and if we want to empower ISPs and consumers, there need to be electronic ways for them to see, sort and decide what they wish to do to the e-mail.

Now, the bulk senders, the NAI e-mail service providers, deserve a lot of credit for the Lumos proposal. It's a very high standard they're talking about. They're talking about identifying themselves when they send e-mail at a secure level with a digital signature, as well as DNS, and asserting what type of e-mail it is. That is a very, very good plan.

Additionally, they may want to do a relationship permission. At this level, we should know who the people are and there should be a cost to that so it can start to change the economics of Spam, who are the people who are sending e-mail? And it's very important that there be a standardized opt-out. We're hearing from our friends at the filter companies and the ISPs, and these are things that can happen today.

At the highest level, if things that would create a visible seal for the consumer, and that's where our trusted sender program plays, there needs to be very, very sure ID. And visible assertions that should be made that there is a way to opt out that can be trusted, that there is a link to a privacy policy, that there is a dispute resolution mechanism in force. A trusted sender is with TrustE, which is a good body for industry self-regulation.

And the last thing I want to say, with this program that's an open standard and involves many, we can do this without breaking the existing protocols or waiting -- Paul's work is very important at the ASRG, but it takes time to change protocols at that level. We have existing protocols for SMTP with X headers, and we have existing protocols with X509 certificates that can change this problem very quickly.

I just wanted to let you in on some information we know. There's an ROI for trust. We have done some studies with the program. We cannot name it, but there are higher open rates. There are higher click-through rates and there are lower opt-out rates. But more importantly, look at the numbers for the trust ROI. Trust pays for people, and as Commissioner Swindle said earlier today, we need to do something that will fundamentally change this equation in the short time. Steps that don't go from the legal responsible sender, okay, to the actual recipient and their ISP, with confidence in who they are and what they're sending, are only half steps. The mailers are very -- the service providers are willing to go there, and the advocates who supported this plan this morning, and we thank them, are willing to be part of this as well.

So, that is our pitch for this. This is not an exclusion to anything that's happening here, but it's the first step where we come together and make technology a royalty-free open standard to enable all this to happen. Thank you.

(Applause).

MR. HUSEMAN: John Levine, your thoughts on this proposal?

MR. LEVINE: I've actually looked at in some

detail, because the CAUCE board -- I'm a member of the board of CAUCE, and we have endorsed the concept, not the product or the implementation or anything, but the concept of being able to put assertions on e-mail like this that you can test and you can actually determine whether a mail purports to be bulk or doesn't purport to be bulk and who is making the assertion.

And although, like nothing else, it's no magic bullet. I was actually surprised. It looks really good.

MR. SCHIAVONE: Yeah, how about that?

(Laughter).

MR. LEVINE: And I think that something like this that can be layered on top of mail and particularly could work with laws that could -- assertions in mail about what the mail is, if if were -- that would make it easier to enforce laws that could sanction you if these statements you made about the mail you sent weren't true.

MR. HUSEMAN: David Berlind, do you have a comment on this proposal?

MR. BERLIND: Yeah, I think that -- first of all, I want to commend every organization that steps forward and says certify us, give us a hall pass based on our -- some best practices that we've advanced. But you should be aware of the fact that there are probably 20 such organizations, all who have advanced a separate set

of best practices. There's no uniformed set of these, and that any time I hear the words dispute resolution, first of all, I -- you know, as a technologist, I say that's a human process, it's not possibly scalable on a global basis, number one; and number two, it implies a great degree of subjectivity.

And, so, you know, I think to the point of things like attestable things, like a verifiable -- I saw it in the diagram -- a verifiable opt-out link, that there should be no one set of best practices that speaks on behalf of me and what I want in my inbox. In fact, these best practices are proposed by the organizations who represent a high-volume e-mail constituency. They never consulted with me. And, so, it's kind of like the fox watching the hen house.

I think that ultimately what I want is a set of things that can be tested, like an unsubscribe link, that I can say well, if the e-mail has an unsubscribe link or something that terminates my relationship and it functions, then go ahead and let it through, but if it doesn't, then don't let it through. But I worry about any system that's based on best practices when currently we have no agreement on best practices within the borders of the United States and we certainly will never get an agreement internationally.

MR. HUSEMAN: Vince Schiavone, your response?

MR. SCHIAVONE: That's why we suggested there be an open standard of the ability to make assertions that will vary, because David's absolutely right, it's up to him what he wants to accept, and it's up to the ISP and their acceptable use policy. But if we have a standard way to make these assertions, then they can happen in a scalable way. And one other quick thing I'd like to say, we do have experience that with e-mail, much of dispute resolution, a very, very high percent of it, is automatic, it can be handled electronically, because mostly people want to come off the list, and they want to know that that will actually happen.

MR. HUSEMAN: Steve Atkins, any thoughts on this proposal?

MR. ATKINS: Of the various trust proposals I've seen, it's one of the better fleshed out. I'm not entirely convinced that trusted sender is the answer to everything, but it is a good way of reducing false positives if it's maintained properly.

MR. HUSEMAN: Steve, you also have your own proposal to change the protocol of e-mail. Can you briefly describe what you envision as solving the Spam problem.

MR. ATKINS: Well, watching a lot of the

discussions over the past couple of months, I've seen an obsession with putting more and more band-aids and duct tape around SMTP, and there's good reason for that. Rolling out a new protocol to replace SMTP altogether, the deployment issues are horrific. It would take many, many years. But that doesn't mean that it's not possible to use a different protocol in addition to SMTP for some of the applications that SMTP is currently used for.

So, I looked at some of the problems with solicited bulk e-mail, newsletters from a company that you've actually opted into and want to receive and saw a couple of problems. One is that an awful lot of them get caught in Spam filters because they look Spam as far as the rules-based system are done. A properly done newsletter will have an opt-out link. A very well known and widely used Spam filter considers an opt-out link to be a sign of Spam, so a lot of newsletter get erroneously filtered, a very high fraction of false positives in Spam filters are solicited bulk e-mail.

The other problem related with that is that the recipient has lost all control. They give their e-mail address to the sender, and then they have no control over what happens with it. The sender can sell it on; the sender can refuse to unsubscribe them when asked. They're relying on the integrity of the sender to control

their mailbox.

Because of that, they often fear to sign up for them. They're wary of signing up for newsletters, because they don't know what will happen when they do. They don't know whether they'll be able to unsubscribe, so I've spent the past few days fleshing out a short discussion document for an alternative protocol that you'd run in parallel with SMTP that any sender could choose to use in addition to their bulk mail distribution; any recipient could choose to use in place of their normal mail client or as part of their normal mail client, whereby instead of them sending their e-mail to address to the sender of the newsletter and the sender then starts sending it, instead the recipient fetches the newsletter from the publisher, and that way they have all control over when it's sent and when it isn't sent, and if they're subscribed to 20 different newsletters from 20 different publishers, they're all administered in the same way, from a single screen on a single client. The full details are pretty simple.

It's the sort of protocol which could be prototyped in a couple of days. It could be made, you know, deployable within a month or so. If anyone's interested to talking about it, it's available up on my website at word-to-the-wise.com. And there's a dozen or

so copies on the table outside.

MR. HUSEMAN: Ryan Hamlin from Microsoft, what are the practical difficulties of any protocol change, such as the one Steve Atkins just described?

MR. HAMLIN: So, I don't -- you know, specific to Steve's -- I would love to look at it. I haven't had a chance to really look at. I think that Steve said it right, I mean, the implementation -- there's a lot -- there's a lot of really good proposals, and Vince's is one and NAI's Project Lumos is yet another. The devil's kind of in the details in really understanding how long it's going to take to roll this out.

I'm a strong believer in an incremental approach and that we are going to learn in kind of a trial by error, so taking the approach of something and trying it and seeing if it makes an effect, what kind of an effect it does have and if it does, roll it out broader, and then going back, and not trying to build, obviously the one-all solution today.

MR. HUSEMAN: John Levine, your thoughts on the practical realities or difficulties of any protocol changes?

MR. LEVINE: Getting rid of SMTP isn't going to happen for decades, if ever. But Steve is absolutely right, that for certain kinds of transactions, there are

other alternatives. I mean, mail is fundamentally a rotten way to send the same message to a million people. You're much better off doing that with -- over the web. You know, and if you can sort of remind the million people that here is a URL to go to to look at your newsletter, that's much -- you could concoct a scheme that would be much more resistant to abuse. You would waste much less bandwidth, because people would actually fetch the text of the newsletter when they were prepared to read it. And you could run something like that in parallel with e-mail.

You could tell people like here's your newsletter toolbar, which is automatically set up to kind of light up the buttons when there's a new issue ready to look at. And Steve is absolutely right, that sort of thing can be built on top of existing alphabet soup things like XML very quickly and could be quite useful as a way both to manage your subscriptions and to push back a whole bunch of Spam-like issues.

MR. HUSEMAN: David Berlind.

MR. BERLIND: Well, one thing about just that particular proposal is that e-mail is by nature a store and forward technology. There are millions of people who download their e-mail to their system and then read it later on an airplane. And, so, if I got some sort of

stub of an e-mail that said okay, now, if you want to read this newsletter fetch it, but I'm on an airplane where I can't get it, that would be problematic. There are probably ways around that, but that would be something that has to be addressed.

I absolutely agree that this has to be addressed at a protocol level. And I'll just give you another suggestion or another idea that happens at the protocol level, which is to take the notion of opt-out links completely out of the control of people who send e-mail to me or anybody else and build it into the protocol. Unsubscribe really means terminate relationship. The protocol right now, you know, in your e-mail client, you know, you have a send button, you have a reply button, why not a terminate relationship button? And when the e-mail arrives into my inbox, my inbox goes to check to see if the sending system will correctly respond to that command, and if it will not respond to that command, then it doesn't let the e-mail through to me.

It also provides an interesting test for legislators to say, hey, have you disabled this part of the protocol, it's kind of like disabling your odometer, you broke the law. Okay, that part of the protocol cannot be disabled, you have to respond to a terminate

relationship command.

And, so, I think there are plenty of really interesting things that can be done at the protocol level that serve as a pass-fail way of not eliminating the Spam problem from a technological solution but also from a legislation solution.

MR. HUSEMAN: I'm going to open the floor to questions now. This gentleman over here. Wait for the microphone, please.

MR. ROYSTON: Clifton Royston, LavaNet. I think we've just seen a great demonstration of why it's hard for the ASRG to make progress, because what Paul Judge, to his great credit, is doing has been managing for the last three months or so, more actually, succession of really clever, intelligent ideas like this from many very bright people, proposals like we've just seen from Vince, Ryan, Steve, David, about every three hours over the period of the last three months, there's a lot of good ideas out there, and I -- to be honest, I think some of the grilling that was directed at Paul Judge representing the ASRG in the context of how many weeks from now are you going to give us a solution to Spam, reflect a misunderstanding of what -- not only how the IETF works but what the distinction is, which is going to make no sense to many people who are between the

IETF -- Internet Engineering Task Force and a research task force. I understand all these issues that keep getting raised with each proposal that comes up is this going to work a year down the road, two years down the road? What will this break? Paul has been tasked with making sure that what gets proposed is good for the next 20 years once it's deployed and that's --

MR. HUSEMAN: So, your point is that there are great difficulties in coming up with these solutions and that the process of sorting through all these ideas is difficult, which I guess leads me to a question of all the panelists. Will any -- will there be any technological solution or structural change to e-mail that will stop Spam?

MR. BERLIND: I would say the answer to that is the day that everybody decides to work together, and I mean the six different communities, we'll have a solution on very short order, as long as they commit to that.

MR. HUSEMAN: Let's keep it brief. Vince Schiavone?

MR. SCHIAVONE: Absolutely. As soon as we add security and trust to e-mail, we can get to the solution that excludes it. It will always come in, but it will be treated much differently than trusted e-mail.

MR. HUSEMAN: John?

MR. LEVINE: Will there be changes? I think the answer is yes, because when the three big gorillas -- you know and say that, you know, you have to play by our rules to send us mail, the rest of us will have to do what they say. And it -- that's true, but it remains to be seen whether it's Vince's proposal or something else, whether it will actually deal with the issue in ways that Spammers can't get around.

MR. HUSEMAN: Ryan Hamlin?

MR. HAMLIN: Not as concerned as much about the forum, I think everyone has to have a seat at the table, which we will drive forward with. As an industry now it's very apparent, as well as being, I guess, one of the gorillas, I would say it's -- you know, we have high incentives to solve this problem. Not only is it the number one concern our consumers have, it is costing us millions of dollars a year to do that. So we are highly incentive to move forward on these.

MR. HUSEMAN: Matt Sarrel?

MR. SARREL: There will eventually be a solution. I think that, you know, in very vague, very quick terms, it will rely on knowing who the -- an authenticated sender, an unmodified e-mail that clearly states what it is and the recipient having an easy and accurate way of opting out.

MR. HUSEMAN: Dan Tynan?

MR. TYNAN: If you're speaking purely as a technological solution, then, no. Technology in combination with some form of, hopefully, smart legislation and perhaps private right of action combined may do it. But just providing technology will not get rid of the bad actors.

MR. HUSEMAN: Paul Judge?

DR. JUDGE: It's a simile with Daniel, that the solution is definitely one that's technical and legislative and so on, but on the technical side, I have not seen a silver bullet. I believe I've seen, you know, every proposal for anti-Spam system, but I haven't seen a silver bullet. I've seen a number of systems that crafted together carefully will tremendously help us to control the problem, and I think again it's about collaboration, people deciding that we're going to work together and come to some consensus and work together to deploy this.

MR. HUSEMAN: And one point of clarification about the process, correct me if I'm wrong, but your Anti-Spam Research Working Group will then make recommendations to your Internet Research Task Force, which is a sister organization of the Internet Engineering Task Force, which will -- is then the

organization that sets the standards for the internet. Is that correct?

DR. JUDGE: So that's -- that's correct, one form of deliverables is recommendations on a solution set and that could be made as recommendations to the IETF, but in reality, there's really a couple of paths to solving a problem, and one is that traditional standardization approach. And that does take some time. But there's also de facto standards, they're sitting down and writing code and, I mean, code talks, and we're not confused about that, so that's why we're forging relationships between -- for example, in the Spam research group, every company that creates an anti-Spam product participates in that group. So, if you have consensus among that group and you begin to have consensus between those groups and the ISPs, then we can have things that are out there and out there working in the short term.

MR. HUSEMAN: Steve Atkins, to get back to the question, will there -- or is it possible to have a structural solution or technological solution to Spam?

MR. ATKINS: I don't believe a purely technological solution is possible, because as several people have mentioned, SMTP is not going to go away. For decades there will be people who will want to send my e-

mail over SMTP, so there will have to be some way for them to talk to me, even if I'm primarily using a different protocol. But I believe a combination of technological fixes and possibly legislation and definitely a lot of social and communication work, primarily between ISPs will happen, and it will happen soon. And the reason I say that is if it doesn't happen soon, in a lot of areas, SMTP mail is going to fall over or get worse. Even filters just push the problem to the ISPs, rather than the recipients. So, yes, there's going to be a technological and social fix soon, because otherwise everything is going to break.

MR. HUSEMAN: One question I had before I turn it back to the audience. We talked legislatively about a do-not-Spam list. Is such a list currently technologically feasible?

MR. LEVINE: I actually talked to Senator Schumer's office about this yesterday. A list of e-mail addresses is not practical. It would be too huge and too impossible to maintain and too onerous. As I said to them, I mean, do you really expect General Electric and Citibank to give you a list of all of their employees, to beg people not to Spam it. On the other hand, if you do it at a higher level, by domain or by putting no-Spam tags on mail servers, I think that would be

technologically implementable. As in connection with an effective do-not-Spam law.

MR. HUSEMAN: Vince Schiavone?

MR. SCHIAVONE: I hope it's not inevitable, but with the -- I'm from Pennsylvania, and our do-not-call list was very popular very quickly. Because I think a do-not-e-mail list would be a very bad idea. It's a different medium, and there are people who forget when they opt out that they also signed up to receive information. There's a lot of confusion.

We do not currently have clear standard definitions of what a newsletter is or what UCE is, and if we need to go a step before that where we have some type of classifications that people can choose to sort by.

MR. HUSEMAN: But does the technology exist to have such a list?

MR. SCHIAVONE: The technology exists to do everything, but just like with Eileen here, if you fund it enough, we can do it, but I still don't think it's a good idea or it will work very well.

MR. HUSEMAN: Paul Judge, would a do-not-Spam list be technologically feasible?

DR. JUDGE: Yes, we have the technology to make it secure and to make if efficient. So, yes, it's

technically feasible. The one question is opt out of what?

(Laughter).

DR. JUDGE: I don't think the answers necessarily are global opt-out of e-mail. I think that you have to get some granularity there or you have to be able to express what you're expressing the lack of consent for, what type of communication do I not want to receive. And then perhaps there's multiple opt-out lists, and then you begin to have something that's useful.

MR. HUSEMAN: David Berlind?

MR. BERLIND: I think that such a list is just totally impractical, and the reason is that it relies on the fact that you have to define Spam, and that problem will never get solved. And I think that the real answer, if you're looking for some form of list management, would be a permissions data base, which basically allows me to track who I've given my permission to and who I have not and then when somebody sends me something, it better come with that permission attached to it.

MR. HUSEMAN: Steve Atkins, is a do-not-Spam list technologically feasible?

MR. ATKINS: Do-not-Spam is so ill-defined that no, it's not feasible. What's really meant is a list of

e-mail addresses or domains which do not want to receive some specific type of e-mail. Let's call it unsolicited bulk e-mail that is well defined. Is it technologically feasible? Yes. But at that point it becomes merely a legal nicety, because the last time such a list was created, one of the first things that happened was the whole of aol.com opted out. At that point, it's going to be used purely as a pretext for legal action, rather than as anything that really gives choice to the end-user, because given the choice, the end-users don't want unsolicited bulk e-mail, except for a very tiny fraction.

MR. HUSEMAN: Let's open it back to questions from the audience again.

MR. HUGHES: So, we're on the topic of do-not-e-mail lists. So, the question for the panel is doesn't a do-not-e-mail list create the richest source of e-mail addresses for Spammers? And doesn't the security around that list become an enormous problem? It just seems to me that that makes it an absolutely horrible idea.

MR. HUSEMAN: John Levine?

MR. LEVINE: You're absolutely correct, and that's one of the reasons why I suggested to Senator Schumer's office that doing it by domain or by server is much more practical, because then you're not listing individual addresses; you're only listing domains which

are already publicly known.

MR. HUSEMAN: Vince Schiavone?

MR. SCHIAVONE: Yes, it is a security nightmare. We've heard things of a hail storm where all data was stored in one particular silo. It's a very bad idea. But David Berlind suggesting that permission, whatever it be, whether it's unsolicited, whether it's existing relationship, can go with each and every e-mail.

MR. HUSEMAN: Paul Judge?

DR. JUDGE: So, I believe, yeah, if you implement it in a naive manner, then it's insecure, but there's very basic technologies available to implement a secure data base, simply an e-mail address and a data base of hashes of e-mail addresses. You'd have a one-way hash function of e-mail addresses, then you allow someone to check whether or not an e-mail is in that data base or not, without ever having access to what e-mail addresses are in there.

MR. HUSEMAN: Steve Atkins?

MR. ATKINS: What he said.

(Laughter).

MR. ATKINS: An e-mail opt-out list is a bad idea, but the security issues are not the reason it's a bad idea. They're easily resolved.

MR. HUSEMAN: The gentleman in the striped

shirt, right there.

AUDIENCE MEMBER: There was a solution that was mentioned at the beginning, and I don't think it was paid enough attention to, maybe because it's a good solution for users. I think it's also a good solution for those who send permission-based e-mail, and that is a token-based system, so the idea is that you take an e-mail address, and we understand that now to have two parts, the part before the @ sign and the part after the @ sign. What we can do is put in there a token, and this already exists in several ISPs. In the ISP I use, it's there. So, you have the first part, a plus sign, the token, the @ sign, and then the domain.

Now, that gives -- I think that solves the opt-in problem, because you've opted in because I've given you a token to get into my inbox. So, I think that's a good solution for those who want permission-based marketing. I think it's a good solution for users because it gives them virtually unlimited number of e-mail addresses that they can use, and they can filter on.

MR. HUSEMAN: Any comments from the panel on that question? Vince Schiavone.

MR. SCHIAVONE: E-mail's big and fast, and there's a lot of scalability issues, and disposable e-mail addresses are very good for technical people like us

in this room, but most consumers cannot handle it.

MR. HUSEMAN: One more response and then one more question. Steve Atkins?

MR. ATKINS: They're what I use, but they are not really appropriate for a lot of end-users. Managing the data base of them gets a little complex.

MR. HUSEMAN: Then Jason Catlett in the back, Jennifer.

MR. CATLETT: Thanks, Jason Catlett from JunkBusters, and I'm against Spam, and I encourage filtering by ISPs, but I don't feel entirely comfortable with the prospect of the three gorillas, as John Levine called them, getting together and running the post office, particularly when the three gorillas each have a large catalog business of their own. Is there anyone else who is worried about that?

(Applause).

MR. HUSEMAN: John Levine first.

MR. LEVINE: I wasn't proposing this as a desirable situation, but I was proposing it as one that was one that was not altogether implausible.

MR. HUSEMAN: Ryan Hamlin?

MR. HAMLIN: Yeah, and I think I was pretty clear, I mean, from the get-go, we've said all along that every group needs to have a seat at the table. We

certainly don't intend to exclude anybody. We are highly incentive, because we are the ones that are opening our checkbooks quite a bit today and spending millions and millions of dollars, but certainly everyone will have a seat at the table and a voice at the table. That was not the intention at all.

MR. HUSEMAN: We have one more minute. I'm going to bleed every last second out of you for this forum, so one more question, and let's have it, Jennifer, from the gentleman in the back there.

AUDIENCE MEMBER: I had a couple of questions, actually. One is --

MR. HUSEMAN: Keep it very brief, please, you have about 15 seconds.

AUDIENCE MEMBER: Okay, talk about the combination of technology and legislation, but I wonder if anyone could talk about the combination of technology and economic incentives? There's Shred, there's Vanquish, there's Bonded Sender. There's a lot of proposals there. And then just regarding the do-not-e-mail lists, I still would like to have someone explain to me how there's not an easy directory, harvest attack on such a do-not-e-mail list.

MR. HUSEMAN: Does anyone want to address the directory harvest attacks?

MR. LEVINE: Talk to one of us later and we can explain the technology. As far as e-postage, I have yet to see an e-postage system that looks even faintly implementable. So, at this point, it's just vapor-ware. I don't think it's a practical approach.

MR. HUSEMAN: Okay. Steve Atkins, you have 15 seconds.

MR. ATKINS: Economic incentives, I-import, bonded sender, looks viable, maybe-ish in some cases.

(Laughter).

MR. HUSEMAN: Great. Thank you. Now I'm going to introduce Eileen Harrington, who will help conclude us off.

(Applause).

MS. HARRINGTON: Isn't Brian wonderful?

(Applause).

MS. HARRINGTON: He's been working around the clock on this for weeks, and here he is bleeding the last second out of the forum. I can't believe it. I would have been running out of the room by now, I think.

One of your colleagues said to me a minute ago, it feels like this has been going on forever. I think some of us wish that it could go on for a few more days, because it's been so rich. And I think that we've saved the best for the last, and with that I certainly don't

mean me, and I don't even mean my boss, Howard, who I'm about to introduce, but this was really a wonderful panel and very rich in information, in thought, in idea, in challenge, and I want to thank all of you, and all of you. This is sort of the end of Survivor, except there's so many people left on the island.

(Laughter).

MS. HARRINGTON: I'm just amazed. I'd like to introduce Howard Beales, who is my boss and our boss and the Director of the Bureau of Consumer Protection at the FTC. As Commissioner Swindle said this morning, at the FTC, it's all about consumers. And Howard is the guy who is responsible for carrying that flag. So, to wrap things up for us, Howard Beales.

(Applause).

MR. BEALES: Thanks, Eileen. They always schedule me at the end of these workshops, in case there is nobody left.

(Laughter).

MR. BEALES: They figure commissioners might be upset, but the bureau director, well, that's okay. I want to -- we have come to the end of what I think has been a very productive and a very exciting forum over the last three or four days. I want to thank all of the panelists who volunteered their time and expertise and

everybody in the audience who volunteered their time and expertise to help educate us about the complexities and the realities of the Spam problem.

I also want to thank Chairman Muris and the commissioners who participated in the forum, Commissioner Swindle, Commissioner Thompson, in particular, for sharing their deep commitment to addressing and responding to the many questions and concerns that are out there about Spam.

And I want to thank the staff, who was really tireless in putting together an outstanding workshop.

(Applause).

MR. BEALES: It's really easy to say, and I've learned to say it very well, let's do a workshop.

(Laughter).

MR. BEALES: And it's very hard to actually do, and they've done an outstanding job. Over the last three days, we've heard from a number of people with different perspectives on addressing the Spam problem. That diversity of opinion has provided for a lively debate, a very informative and I think a very informed discussion on a great many issues.

The panel discussions I think have clearly confirmed there isn't a simple magic solution, sad as that may be, but they also illustrate that there are many

directions that we can take to try to protect e-mail for consumers and for commerce. Many panelists discussed how the swelling tide of Spam harms consumers and businesses by imposing significant costs on them. Consumers find themselves confronting unseemly images, spending time deleting unwanted messages or not receiving valued e-mail in lieu of receiving e-mails that promise immediate wealth or a cure-all health care.

Businesses lose productivity because employees spend time deleting unwanted e-mail. They spend more money putting systems in place that will diminish the amount of Spam that gets through their filters. Further, there are costs, both large and small, that Spam imposes on internet service providers.

Our panelists indicated that although the costs are currently significant, they're going to give way to a far greater harm, the loss of confidence in the powerful communications medium of e-mail, and quite potentially decreasing participation on the internet. We are at risk of killing the killer-app.

The panelists also reaffirmed, there's a role for continued aggressive law enforcement by the FTC and other law enforcement authorities. We're certainly going to continue to pursue vigorous enforcement against those who threaten this communications medium, and the

marketing tool, by sending deceptive e-mail. We'll also continue our efforts to educate consumers and businesses in the steps they can take to decrease the amounts of Spam and to recognize deceptive Spam when they see it. We'll continue to study the issues; we'll continue to take innovative steps to try to remain at the forefront of stopping deceptive Spam and providing meaningful consumer and business education. For example, you can expect action from the FTC on the open relay issue in the very near future.

One final housekeeping note, because of the overwhelming interest in this conference, and because of the turnout, I realize that many of you may not have had the chance to make a comment or ask a question. We invite you to supplement our record until May 16th. The details and the instructions for doing so are on our web page, at www.ftc.gov/bcp/workshops/Spam.

And speaking of this website, we're always interested in sharing the information on it with consumers and businesses. If you'd like to join us in this effort, then please contact Charles Lawson in our Office of Consumer and Business Education, at the risk of having him overwhelmed, he's at clawson@ftc.gov.

Again, we feel strongly about the issues concerning Spam, and I know that many of you are

passionate about these issues as well. I'm glad that we've been able to host this thoughtful and productive forum as a building block to address many of these issues. My colleagues and I look forward to working with you in the future. Thank you again for devoting your time and effort to the forum, and thank you for staying until the very end.

(Applause).

(Whereupon, the hearing was concluded.)

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: May 2, 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 20, 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