

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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

| | |
|--|----------|
| Potential Solutions to Spam | Page 2 |
| International Perspectives | Page 107 |
| Technological Solutions to Spam/ Structural Changes to E-Mail | Page 239 |

P R O C E E D I N G S

- - - - -

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

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

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

21 **(Applause.)**

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

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

5 **(Group laughter.)**

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

18 **(Group laughter.)**

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

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

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

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

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

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

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

12 MR. WELLBORNE: Yes.

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

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

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

25 The Europeans had come over fleeing Germany;

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

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

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

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

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

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

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

12 **(Group laughter.)**

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

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

1 long time ago -- and that challenge is Spam.

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

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

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

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

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

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

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

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

1 make some progress. That's a fact.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 sneaking suspicion.

2 **(Group laughter.)**

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

8 **(Group applause.)**

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

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

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

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

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

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

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

13 **(Group laughter.)**

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

19 **(Group laughter.)**

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

25 We have a busy day ahead of us and as my

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

5 Thank you very much.

6 **(Applause.)**

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

11 **(Group laughter.)**

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

16 **(Group laughter.)**

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

21 **(Group laughter.)**

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

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

5 **(Group laughter.)**

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

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

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

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

25 Chuck Curran, down on the end, is the Assistant

1 General Counsel at America Online.

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

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

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

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

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

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

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

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

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

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

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

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

1 Washington was the second state to pass legislation in
2 this area. As with a lot of consumer protection-type
3 issues, the states are usually the place where these laws
4 first get passed. And what happens is you get
5 essentially what becomes a patchwork of laws across the
6 country. This happened in telemarketing, it happened in
7 900 numbers, it happened in credit reporting, and on and
8 on. And what happens eventually is that those who are
9 regulated eventually come to Congress and say, please,
10 please legislate, because we can't deal with the
11 patchwork of laws. And I think that's part of the
12 impetus for this Federal legislation that we're seeing
13 now.

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

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

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

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

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

12 MS. HARRINGTON: Okay. David Kramer?

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

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

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

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

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

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

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

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

4 MS. HARRINGTON: Thanks. Ray?

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

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

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

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

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

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

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

16 MS. HARRINGTON: David?

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

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

1 solution.

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

3 MR. SORKIN: Yes.

4 MS. HARRINGTON: John?

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

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

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

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

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

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

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

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

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

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

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

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

21 Who would like to start?

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

23 MS. HARRINGTON: Okay.

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

1 it's labeling -- why do I care?

2 MS. HARRINGTON: Okay.

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

5 MS. HARRINGTON: The Tajikistan Perspective.

6 **(Group laughter.)**

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

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

10 MS. HARRINGTON: The Seattle Stand.

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

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

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

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

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

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

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

1 action.

2 MS. HARRINGTON: Some of my colleagues in this
3 room -- Jennifer, Marc, Lisa, others -- spent 18 months
4 going around the country training state and local
5 enforcers on internet investigation technique. We got a
6 lot of interest, we trained, I don't know -- Marc --
7 1,750 local and state enforcers on how to do this kind of
8 investigation. And, so, for us there's a little bit of a
9 disconnect between the effort to put in that kind of
10 training effort and the lack of enforcement at the local
11 level of these laws.

12 Is there more that we can do to encourage
13 enforcement?

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

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

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

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

10 MS. HARRINGTON: Okay.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 fraudulent and the --

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

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

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

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

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

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

7 MR. RICHTER: Eileen?

8 MS. HARRINGTON: Yes.

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

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

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

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

11 MS. HARRINGTON: Ray?

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

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

1 domestically.

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

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

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

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

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

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

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

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

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

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

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

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

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

25 Just anecdotally, my fax machine at the Federal

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

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

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

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

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

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

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

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

22 Jerry?

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

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

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

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

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

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

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

9 MR. RICHTER: I'm for private right of action
10 in a court of competent jurisdiction, and what I want to
11 do is allow the citizens to get into court without having
12 to find an attorney and without having the attorneys
13 profit. So, in most claim courts right now, their
14 limitation, I think, is about \$5,000 -- maybe some states
15 a little bit less -- but I think everybody is leaning
16 toward the \$5,000. I don't think we're talking about a
17 \$5,000 fine, so where we're talking in the neighborhood
18 of \$250 or \$500 per e-mail, you know, as a violation, let
19 the consumer be able to go into a small claims court,
20 file a \$30 fee, and have their day.

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

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

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

13 John?

14 MR. PATRICK: I think we're --

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

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

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

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

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

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

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

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

5 MS. HARRINGTON: Okay, Ray?

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

8 **(Group laughter.)**

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

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

25 MR. RICHTER: Eileen?

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

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

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

17 Paula, would you like to start on that?

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

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

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

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

8 MS. HARRINGTON: And why not?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6 MS. HARRINGTON: What are those?

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

9 MS. HARRINGTON: Why?

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

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

18 So, we think those are good places to start.

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

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

1 MS. HARRINGTON: What do you like about it?

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

6 MS. HARRINGTON: Is the standard too high?

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

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

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

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

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

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

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

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

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

20 MS. HARRINGTON: Okay. Thank you. David?

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

25 **(Group laughter.)**

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

6 MS. HARRINGTON: Theft is a strong term.

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

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

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

1 **(Applause.)**

2 MS. HARRINGTON: Okay.

3 MR. PATRICK: I want to strongly agree.

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

6 **(Group laughter.)**

7 MS. HARRINGTON: John?

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

17 MS. HARRINGTON: David Sorkin?

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

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

24 **(Group laughter.)**

25 MR. SORKIN: I would probably draft a

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

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

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

1 MR. EVERETT-CHURCH: Eileen?

2 MS. HARRINGTON: Yes, Ray.

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

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

25 Can you think of some sort of statutory scheme

1 that would be less likely to be immediately obsolete?

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

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

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

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

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

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

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

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

18 MR. CURRAN: The volume issue is a very
19 difficult issue because, certainly, every day, seven by
20 24, the Spammers are out there on a technology side
21 testing whatever filter -- if you say the number is 10,
22 they're at nine; if you say the number is 100 -- and the
23 nature of SMTP -- mailing protocols -- allows mail
24 transmissions to be broke up into so many little packets
25 that mail, as sent by sophisticated Spammers today,

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

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

9 MR. PATRICK: I disagree.

10 MS. HARRINGTON: Who said that?

11 MR. PATRICK: John.

12 MS. HARRINGTON: John?

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

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

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

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

5 **(Mixed applause.)**

6 MS. HARRINGTON: Ray?

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

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

25 MS. HARRINGTON: I see people are getting a

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

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

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

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

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

17 MS. HARRINGTON: Okay, thank you.

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

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

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

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

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

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

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

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

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

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

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

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

1 MR. KRAMER: Yeah, it isn't, is the short
2 answer to the question. The problem is almost exactly
3 the same. I would suggest that it's far worse, in fact,
4 in the context of e-mail, as I did previously, and I
5 think the solution that we came up with as a society in
6 1991 here ought to be the solution that we come up with
7 to this problem in 2003.

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

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

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

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

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

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

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

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

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

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

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

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

21 The other component is --

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

1 Spammers.

2 MR. RICHTER: Well, I think --

3 MS. HARRINGTON: Do you like this idea?

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

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

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

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

22 **(No response.)**

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

25 Let's turn to the Schumer approach, which

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

3 UNIDENTIFIED SPEAKER: Lucky you.

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

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

11 **(Group laughter.)**

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

14 MR. SORKIN: Preferable anybody but ICANN.

15 **(Group laughter.)**

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

17 MR. PATRICK: Eileen?

18 MS. HARRINGTON: Yes? John?

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

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

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

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

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

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

17 **(Group laughter.)**

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

21 MR. CERASALE: Well, unlike the telephone,
22 where a do-not-call-list works, has worked in the states
23 and so forth, and even the DMA list has been around since
24 '85, where the fraudulent people were in telephone
25 marketing or on the fringe, it's the legitimate marketers

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

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

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

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

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

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

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

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

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

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

19 MS. HARRINGTON: Okay.

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

1 and FedEx and Airborne. So --

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

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

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

19 MS. HARRINGTON: Pardon me?

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

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

25 MR. PATRICK: Well, it's --

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

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

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

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

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

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

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

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

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

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

11 MS. HARRINGTON: Ray?

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

16 **(Group laughter.)**

17 MS. HARRINGTON: David?

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

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

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

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

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

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

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

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

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

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

14 MR. CERASALE: Should apply to all.

15 MS. HARRINGTON: Chuck?

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

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

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

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

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

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

12 MS. HARRINGTON: Ray?

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

25 MS. HARRINGTON: Okay. Steve Richter, should

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

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

6 MS. HARRINGTON: Okay, David?

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

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

17 **(Group laughter.)**

18 MR. PATRICK: Eileen?

19 MS. HARRINGTON: Yes?

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

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

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

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

17 MR. HUSEMAN: Yes.

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

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

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

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

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

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

25 MS. HARRINGTON: And doing that intentionally

1 would be the intent to falsify?

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

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

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

19 MS. HARRINGTON: Thoughts on criminalization?
20 Paula?

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

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

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

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

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

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

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

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

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

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

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

1 members as they write and draft?

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

4 MR. SORKIN: I'll go first.

5 MS. HARRINGTON: Sixty seconds.

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

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

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

12 MS. HARRINGTON: John?

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

15 **(Group laughter.)**

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

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

1 good ideas.

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

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

11 MS. HARRINGTON: Five seconds.

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

14 MS. HARRINGTON: Ding. Next?

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

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

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

8 MS. HARRINGTON: Five seconds.

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

10 MS. HARRINGTON: Excellent, Dave.

11 **(Applause.)**

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

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

17 **(Group laughter.)**

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

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

1 make money by sending out big volumes -- maybe getting a
2 1 percent return -- it makes sense for him to keep
3 Spamming. But the minute he has to face criminal
4 penalties, statutory damages, the threat of big lawsuits,
5 he'll stop. It's a dollar-and-cents issue, and if the
6 balance is on the side of fear of enforcement, the
7 Spamming will stop.

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

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

22 MS. HARRINGTON: Okay. Next? Chuck?

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

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

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

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

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

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

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

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

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

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

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

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

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

5 **(Group laughter.)**

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

10 Now, Commissioner Thompson?

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

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

22 MS. HARRINGTON: Very good question.

23 Panelists? Ray?

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

1 Commercial E-mail has been working on this issue since
2 1997, when we were founded. We felt that it was a
3 problem then and a growing problem, and that the dire
4 predictions we made and were laughed at for have,
5 unfortunately, come to pass.

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

9 MS. HARRINGTON: Steve?

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

18 MS. HARRINGTON: David?

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

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

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

4 MS. HARRINGTON: John?

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

14 MS. HARRINGTON: Okay.

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

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

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

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

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

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

11 **(Group laughter.)**

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

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

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

25 The second is the state actions and making

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

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

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

25 Furthermore, this actually can extend to the

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

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

10 MS. HARRINGTON: Okay, thanks.

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

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

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

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

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

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

18 **(Group laughter.)**

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

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

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

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

14 **(No response.)**

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

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

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

25 MS. COHN: Yeah. Brian asked whether we needed

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

3 MS. HARRINGTON: No.

4 MS. COHN: Did I misunderstand?

5 MS. HARRINGTON: Yes.

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

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

11 MS. COHN: Oh, I misunderstood?

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

14 MR. CERASALE: My answer was only on
15 commercial.

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

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

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

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

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

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

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

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

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

1 our last audience question.

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

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

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

19 **(Group laughter.)**

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

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

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

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

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

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

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

15 **(Group laughter.)**

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

18 COMMISSIONER SWINDLE: Solve the problem.

19 MS. HARRINGTON: Solve the problem.

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

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

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

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

13 Thank you.

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

17 Thank you, panelists.

18 **(Applause.)**

19 **(Whereupon, a brief recess was taken.)**

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

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

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

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

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

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

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

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

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

12 **(Group laughter.)**

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

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

1 situation in Korea.

2 Total population of Korea last year was around
3 47 million, and about 58 percent of the population, which
4 is equivalent to 26 million, reports that they have
5 access to the internet and use it at least 12 hours a
6 week. And we have, also, around 30 million people who
7 use mobile telephone, hand phone sets.

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

14 The result of a survey of 2,000 e-mail users
15 conducted by KISA last year shows that every user has an
16 average of four e-mail accounts and receives 14 e-mails
17 every day in each account. And eight out of 14, they
18 report, were unsolicited and unwanted ones. So, around
19 60 percent is unwanted ones. This is a rapid increase
20 from 2001 when Spam occupied 44 percent.

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

25 Next, let me move to the regulatory efforts of

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

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

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

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

25 To fight against the technological development

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

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

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

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

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

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

25 Besides the enforcement laws, KISA also

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

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

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

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

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

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

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

20 Thank you.

21 **(Applause.)**

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

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

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

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

12 **(Group laughter.)**

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

15 **(Group laughter.)**

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

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

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

1 have a handout, so please look at it.

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

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

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

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

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

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

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

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

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

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

7 MR. TSUCHIYA: Mostly from --

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

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

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

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

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

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

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

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

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

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

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

21 **(Group laughter.)**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

11 What I'm going to say might seem shocking to
12 you when I describe to you who our association is and who
13 we represent in Australia. As Tom said, we're the
14 national industry body for the internet. We have over
15 300 companies, representing a Who's Who of the internet
16 industry in Australia. They include players like
17 Telstrel (phonetic) Optus, AOL, Aussie Mail, MSN, Yahoo,
18 a lot of the major security and filter providers,
19 Symantec, GenMicro, Message Labs, and others, and, of
20 course, several hundred smaller players as well.

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

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

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

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

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

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

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

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

1 very low threshold, is not going to be effective.

2 And the major point -- and I'm happy to talk
3 about this later -- is how does a so-called legitimate e-
4 mail marketer differentiate themselves from the worst
5 kind of Spamster, and I think opt-out is problematic in
6 that it's too easy for the wrong kind of players to
7 comply with that and you end up with a solution where,
8 you know, the aggregate effect of me getting 30, 40, 50,
9 100 opt-out e-mails in my mailbox every day still
10 constitutes a Spam problem of major proportions.

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

13 **(Applause.)**

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

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

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

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

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

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

25 We began the current review in 2002 more in

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

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

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

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

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

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

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

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

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

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

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

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

1 costs onto consumers.

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

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

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

1 states are working on implementing and so, Philippe.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 the Commission to do that.

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

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

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

1 right, that process is going on now.

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

13 MR. STEVENSON: Thank you. We'll turn now to
14 Marie Georges from France's Privacy Protection Authority.
15 Last year, her agency did a very interesting study on
16 Spam. They set up a Spam box and received, I think, over
17 300,000 Spam and there have been copies out on the table
18 of this report. And France also has some law that, I
19 believe, predates the directive that has been used to
20 address these issues. So, we thought we'd benefit from
21 hearing from the French perspective on this, as long as
22 there are no comments about exportive U.S. culture.

23 **(Group laughter.)**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

22 **(Group laughter.)**

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

1 **(Group laughter.)**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 Commission.

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

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

1 it in the right way.

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

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

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

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

25 MR. STEVENSON: Okay, thank you. Our final

1 foreign panelist is actually from Massachusetts.

2 MS. GRANT: It is a foreign country.

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

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

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

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

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

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

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

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

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

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

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

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

1 MR. STEVENSON: Okay. Peter Ferguson.

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

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

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

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

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

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

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

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

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

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

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

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

9 MS. GRANT: Hugh?

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

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

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

15 MS. GRANT: Okay.

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

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

1 other for cooperation.

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

5 MR. STEVENSON: Thank you. Susan?

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

18 MR. STEVENSON: Peter Coroneos.

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

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

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

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

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

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

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

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

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

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

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

14 MR. STEVENSON: Mr. Tsuchiya.

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

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

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

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

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

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

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

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

9 MR. STEVENSON: Peter?

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

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

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

1 compliance by Spammers?

2 MR. STEVENSON: Would somebody like to address
3 that?

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

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

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

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

6 MR. STEVENSON: Alex?

7 MR. TANDBERG: Axel.

8 MR. STEVENSON: I'm sorry.

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

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

23 MR. STEVENSON: Motochiro Tsuchiya? Susan
24 Grant?

25 MS. GRANT: I just wanted to address the issue

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

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

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

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

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

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

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

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

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

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

13
14
15
16
17
18
19
20
21
22
23
24
25

AFTERNOON SESSION

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

10 **(Laughter).**

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

18 **(Laughter).**

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

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

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

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

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

1 we've heard so much about this morning.

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

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

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

18 **(Laughter).**

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

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

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

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

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

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

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

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

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

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

1 MR. GROMAN: Please talk into the microphone.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 case?

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

4 MR. GROMAN: For how much?

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

9 MR. GROMAN: Right.

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

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

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

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

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

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

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

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

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

13 MR. GROMAN: Okay, thank you.

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

16 MR. GROMAN: Please, please.

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

25 MR. GROMAN: Dietrich, in your cases, your

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

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

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

19 MS. SELIS: The merchant.

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

1 who is it? Who is it that you choose to sue? I guess --
2 I'm going to start with Jon on that, because you have the
3 five new cases, and I've looked at them. It seems to me
4 that your approach is sue everybody.

5 **(Laughter).**

6 MR. GROMAN: But how does that work?

7 MR. PRAED: I don't know that I want to address
8 in particular decisions on any particular case, but I
9 think generally my approach is to sue as big a fish as
10 you can find. I spend probably a majority of my time
11 actually trying to identify characteristics, I call them
12 fingerprints, that constitute a big fish and then target
13 a lawsuit against that individual or group of
14 individuals.

15 And it's really -- you're looking in the end
16 for someone who is sending unsolicited commercial mail
17 using some sort of fraud, and it is a target-rich
18 environment. You talked earlier about Whack-a-Mole.
19 That is the risk that you run, that you are simply
20 playing Whack-a-Mole. I think both on the filter side
21 and on the litigation, you have to systematize what
22 you're doing so that you're not playing Whack-a-Mole.

23 Litigation is critical, though, because I think
24 it is your best opportunity to make the mole pull out his
25 driver's license and actually show you who he is, so that

1 you can thereafter -- he's been bagged and tagged, in a
2 sense.

3 MR. GROMAN: On the issue of who do you sue, if
4 you've got a situation with multiple parties involved,
5 you have a merchant who hires a marketing company, who
6 maybe goes through an affiliate, and then we end up with
7 an individual who sends out the Spam and pushes the
8 button. And the Spammer changes -- or someone along that
9 chain changes the subject line or makes it a deceptive
10 subject line, and you want the big fish who may be on the
11 end. Why is that party liable? Why can they be sued?

12 MR. PRAED: Well, you can make all sorts of
13 arguments to why they should be and why they shouldn't
14 be. In the end, though, Spam conspiracy and assistance,
15 liability for assisting Spammers is not that much
16 different from liability for any other type of illegal
17 conduct. Conspiracy is an old established theory of law.
18 We're not inventing very much law here, really. We're
19 simply trying to take -- in fact, I think one of the best
20 provisions to go after Spammers trespassed the channels.
21 It predates the Constitution. It's not rocket science.
22 The trick is simply getting everyone to agree and
23 understand that these fairly basic concepts of legal
24 principles can be applied in a very new arena in some
25 factually unique circumstances, where identity and really

1 identifying who is the big mole is the real issue.

2 MR. GROMAN: Pete, who do you sue and why?

3 MR. WELLBORN: I'm going to answer that in two
4 parts. I think of Spammers much like Dante's levels of
5 hell.

6 **(Laughter).**

7 MR. WELLBORN: There are ascending levels of
8 egregiousness. At the bottom we have -- we'll call them
9 vanilla Spammers. Those are the ones that send
10 unsolicited commercial e-mail through ISPs that they know
11 forbid that e-mail. It's not spoofed; it's not
12 fraudulent; it's not selling herbal products; it's not
13 selling illegal descrambler boxes. That's your lowest
14 level.

15 Compound that by spoofing and by some of the
16 fraudulent tactics that we've heard about for the last
17 two days. Compound that even more by Spammers who are
18 selling these fraudulent or illegal products. That's the
19 next level. Then there's a top level of egregiousness
20 that the Spammers that are doing all those things and
21 using accounts that are purchased with stolen credit
22 cards or by identity theft to send these e-mails.

23 So, you have those three levels. And as Jon
24 said, what we've done so far is we've gone after the top
25 level, the old saying that the squeaky hinge gets the

1 grease, well, that's the one that we've gone after.
2 After sitting through these panels for the past couple of
3 days, I'm convinced that we need to start going after the
4 lowest level to send a message, because it seems as
5 though there's a fundamental misunderstanding that if
6 you're not spoofing and you're not selling a fraudulent
7 product your unsolicited commercial e-mail is somehow
8 legal or at least a gray area, even if you're sending it
9 through the ISPs of the world who forbid Spam. And
10 that's wrong.

11 If you knowingly send your Spam into an ISP
12 that forbids Spam you're committing a criminal act. You
13 know, there was a lot of discussion this morning about do
14 we -- we need a criminal statute, we need a Federal
15 statute. We've already got them. We've got a criminal
16 statute, it's called the Computer Fraud & Abuse Act.
17 We've got other criminal statutes. It's the state
18 prohibitions against common trespass, the same thing that
19 keeps someone from walking into your house and getting on
20 your computer, keeps them from sending unwelcome Spam
21 into the ISPs. So, let's sue some of these lower level
22 Spammers and send a message that we're not going to only
23 go after you if you're committing credit card fraud --

24 MR. GROMAN: Pete, when you say let's sue, who
25 do you mean? Who's let's?

1 MR. WELLBORN: Let's -- the ISPs that can
2 afford to bear the mantle of the battle, for starters.
3 The Earthlinks who are doing it right now; the AOLs and
4 the Microsofts. For now, with as much cooperation from
5 the government and from law enforcement as we can get, I
6 think these need to be the mantle bearers.

7 MR. GROMAN: Okay, Dietrich, back to you on the
8 same topic. Your client comes into your office with the
9 Spam e-mails, says I've identified who it likely is, I'll
10 use your term, you want to go after, what was it, the
11 low-hanging fruit?

12 MR. BIEMILLER: Low-hanging fruit.

13 MR. GROMAN: Who is that?

14 MR. BIEMILLER: It's somebody who -- first of
15 all, we can't afford to do what Paula does with spending
16 a huge amount of money and getting a minimal return, so
17 we have to -- one of the things unfortunately we have to
18 determine is whether they have money or not to pay a
19 judgment or to pay a settlement. And most of my clients
20 are pretty anti-Spam-active folk, and they go after the
21 highest circle of hell there, and so usually those -- if
22 we can find somebody that combines those qualities and we
23 can identify them, that's a likely target.

24 MR. GROMAN: Stephen, when you're at the end of
25 your investigation, you're making a determination of

1 whose name, what corporation, what individual's name goes
2 on your complaint, what factors are you considering and
3 does jurisdiction become an issue there?

4 MR. KLINE: Yeah, jurisdiction is always an
5 issue for us, but when we are trying to figure out who to
6 sue and why, you know, we -- it's a little -- the Spam
7 cases are a little bit different for us than the rest of
8 our cases, because normally what we're looking to do is
9 get restitution back to consumers. Here restitution is
10 such a tough thing to calculate per Spammer. And then
11 any sort of damages are also tough to calculate.

12 You know, we do consider whether they have
13 money, but what our overall purpose is to do is impact
14 litigation. And if we wind up with an empty judgment but
15 the precedent that we set will steer the industry in the
16 right direction, I think that is the major concern that
17 we have.

18 MR. GROMAN: You mentioned the issue of
19 jurisdiction and you said that's always a factor. Can
20 you explain why that's always a factor?

21 MR. KLINE: Well, because we represent the
22 state. We generally prosecute corporations or people
23 doing business in New York. We have in the past sued
24 people from out-of-state for injuries in New York, but in
25 cases like the Spam cases where we are going to have so

1 many other issues to deal with, and there are Spammers in
2 New York, you know, we try to cut our litigation risk and
3 focus on the bad actors in New York right now.

4 MR. GROMAN: So, if you have an investigation
5 that's open and you ultimately discover somewhere down
6 the road that the Spammer's actually in Texas, what do
7 you do with that case?

8 MR. KLINE: Most likely we'd refer to the Texas
9 AG or the FTC.

10 MR. GROMAN: Have you had luck referring those
11 kinds of cases to other states?

12 MR. KLINE: We haven't had to do that yet.
13 We've -- you know, we've gone to the ISPs and said who's
14 in New York, tell us where they are, tell us what's
15 happening, and we've kind of gotten to pick and choose
16 our cases.

17 MR. GROMAN: Paula, same question. Is
18 jurisdiction a challenge for you or is it really not?

19 MS. SELIS: Well, let me just kind of follow up
20 on what Stephen was saying. When you start out in a Spam
21 case, at least when we start out, we don't know where our
22 defendant is going to be necessarily, true with the
23 Meltzer case. And while in some cases you can pick and
24 choose where your defendants are located, it's harder in
25 a Spam case, you can't, at least not very easily. But in

1 terms of jurisdiction, we haven't run into any issues
2 thus far, though Dietrich has run into jurisdictional
3 issues.

4 We take the position that if you are sending e-
5 mail to the State of Washington and the person to whom
6 you are sending that e-mail has identified him or herself
7 as a Washington resident, then Washington courts can,
8 under long-arm jurisdiction, hear cases involving the
9 defendants. So, so far, so good. I think Dietrich can
10 talk about his case, because his defendant did, in fact,
11 question Washington's jurisdiction, and he got a very
12 favorable ruling.

13 MR. BIEMILLER: They all do. I spend about 80
14 percent of my time litigating jurisdiction, long-arm
15 jurisdiction, so . . .

16 MR. GROMAN: Okay, and just for a background
17 for those of us who are not attorneys in the room, the
18 question really is if the proposed plaintiff is in the
19 State of Washington, and that's where that person may
20 have had their injury, but the Spammer is elsewhere, can
21 Dietrich's client bring the lawsuit in the State of
22 Washington, even though the Spammer may be on the other
23 side of the country and then be forced to litigate the
24 issue there. So, speak about your experiences with that
25 issue.

1 MR. BIEMILLER: Well, that's generally the main
2 question, and they tend to make the same arguments over
3 and over. I mean, why should we have to go to Washington
4 to defend this case, but, you know, the tort occurred in
5 Washington and we exert the long-arm jurisdiction by the
6 statute that we have. It can't exceed the Federal
7 Constitutional issue there about purposeful availment and
8 those kind of issues, but we've been very successful both
9 in superior state court and federal court defending that
10 question.

11 MR. GROMAN: So, you're finding that in your
12 cases the issue of jurisdiction really isn't a challenge
13 or a problem.

14 MR. BIEMILLER: Well, it was a problem for a
15 long time, and I guess Paula can also speak to this, we
16 just recently passed a law specifically addressing
17 jurisdiction because it has been such a problem, for us
18 at least.

19 MR. GROMAN: Okay, turning to the attorneys who
20 represent the big ISPs, I know that AOL's cases have all
21 been filed in Virginia. I think Earthlink's cases have
22 all been filed in Georgia, regardless of where your
23 potential defendants are located. So, let's look to you,
24 Jon, first, and you litigated the Ralsky case. From your
25 perspective, is the jurisdiction just settled, where

1 done, and it's not a challenge anymore?

2 MR. PRAED: I think it was settled before it
3 was even started, but that doesn't keep a defendant from
4 bringing a motion to dismiss, and I think you have to
5 bring a Spam case, wherever you want to bring it, in
6 anticipation of a motion. But I think that it is pretty
7 clearly decided today in the Spam arena. I think the
8 Verizon Online v. Ralsky case was an excellent decision
9 that addressed -- you have a question of forum non
10 conveniens. Can a Spammer be put to the inconvenience of
11 being sued in the state where he actually Spammed, which
12 is a separate question.

13 The real question is did he purposefully avail
14 himself of the protection of the state into which his
15 Spam landed. And a lot of Spammers defend by saying
16 essentially I didn't have a clue. I fired a gun, and the
17 bullet left the gun, and I had no clue as to where that
18 bullet was directed, other than the e-mail address. And
19 I think the court, in the Verizon case, pretty clearly
20 decided that apathy, as to jurisdiction, is not a defense
21 to a personal jurisdiction argument.

22 MR. GROMAN: Okay, so grandma in Oklahoma who
23 sends out 10,000 e-mails and 800 of them actually end up
24 going through an AOL server in Virginia, she's going to
25 be hauled here?

1 MR. PRAED: Well, I have been surprised. I
2 have yet to identify a fraudulent Spammer that actually
3 was a grandma.

4 (Laughter).

5 MR. PRAED: If I got one of them, she's
6 probably going to be driving a Porsche or a Ferrari, and
7 she'll know exactly what she was doing or she won't care.
8 I hear the point. Someone might make an argument that
9 the mere incidental transmission of a small volume
10 doesn't necessarily give rise to personal jurisdiction.
11 An interesting argument, but not one that really has more
12 than a theoretical application in most of these cases.

13 And one correction. AOL has actually filed
14 suit, I think throughout the country. Certainly Virginia
15 has been a common state for suits, but AOL has, in fact,
16 filed I think in California, New York, many other states,
17 in part to try to establish this fairly basic principle
18 across the country.

19 MR. GROMAN: Okay, I want to turn to another
20 issue that our attorneys face, which is causes of action.
21 When you want to bring a lawsuit, there needs to be a law
22 that's been broken. So, what are the causes of action
23 that you are using or advising your clients to use in
24 your complaints? Let's start with you, Pete.

25 MR. WELLBORN: Okay. And one interesting note

1 on the jurisdiction issue, we all owe a debt of thanks to
2 Shirley Jones, the mother from the Partridge Family,
3 whose landmark lawsuit, jurisdiction lawsuit against a
4 writer and editor for The National Enquirer, gave us the
5 most widely cited jurisdiction case when you're claiming
6 the effects test that you can sue here because this is
7 where we got hurt. That's a little hinting aside.

8 **(Laughter).**

9 MR. WELLBORN: Causes of action. I have a
10 laundry list of about 12 or 13 different causes of
11 action, any one of which will carry the day in a typical
12 Spamming and spoofing case. The two most common that we
13 see, as I mentioned earlier, the Computer Fraud & Abuse
14 Act, Federal -- a computer-specific Federal statute that
15 provides for criminal liability in a civil action, as
16 well, if there's been intentional access of a protected
17 computer system that's unauthorized and that causes
18 damage, which that's the very definition of unwelcome
19 Spam coming into an ISP system.

20 Another cause of action that we see a lot and
21 use a lot is common law trespass. It's like I said, the
22 same law that keeps one of you from breaking into my
23 house, coming in and sitting down at my computer and
24 using it, that same general law in each state also
25 prohibits a Spammer from taking unfair advantage of the

1 ISP's computer system and converting the ISP's computer
2 system to the Spammer's benefit.

3 MR. GROMAN: Dietrich, in the private right of
4 action cases that you file, is the cause of action
5 strictly under the Washington Spam statute?

6 MR. BIEMILLER: Typically. I mean, we do cite
7 trespass through chattel, as well, because under their
8 consumer protection act some of the judges have found
9 that they need to have some actual damages in order to
10 enact the treble damages provision of that. But
11 typically we just have this nifty statute that Paula had
12 something to do with, and we use that.

13 MR. GROMAN: Stephen, for your cases for the
14 New York State Attorney General, New York, unlike
15 Washington State, does not have a Spam statute. So, what
16 is the cause of action that you used in your Monster Hut
17 case or other potential cases?

18 MR. KLINE: New York doesn't have a Spam
19 statute, per se, but I consider all of our laws anti-Spam
20 statutes, because the same sort of fraud that's committed
21 on-line has been committed off-line, as well. So, we've
22 been using our deceptive practices statute, which is
23 similar to the FTC act, but we also have a statute,
24 Executive Law 6312 that allows us to prosecute civilly
25 any business who is repeatedly committing fraud or any

1 sort of illegality, which opens the door to all the laws
2 in New York, even common laws. So, we can -- if
3 someone's violating the criminal forgery statute, an
4 administrative statute, common law, all of those fall
5 under 6312 for us. So, I feel right now that I've got
6 all the tools I need to prosecute a Spammer. If they
7 want to give us another one via a Spam statute, which I
8 think they're going to, fine with me.

9 MR. GROMAN: What is the relief that you are
10 seeking in your cases? You mentioned that restitution is
11 not something you're seeking, so what would it be?

12 MR. KLINE: In the MonsterHut case we were
13 seeking penalties. Under our consumer protection
14 statute, we're allowed to seek up to \$500 per violation.
15 And the -- I think the injunctive relief is actually
16 going to be more important than any sort of money
17 judgment. A lot of the -- the two principals in
18 MonsterHut, one fled to Canada; the other one ran down to
19 Florida and is not working. They don't have any assets.
20 So, the money judgments that we're going to get, whether
21 it's penalties or restitution I think are going to be
22 somewhat meaningless. So, I think any sort of injunctive
23 relief is probably the most important thing that we'll
24 get.

25 MR. GROMAN: Paula, turning to your cases and a

1 comment made by Stephen in that -- I know I'm
2 paraphrasing, the money judgment is essentially
3 meaningless or worthless.

4 MR. KLINE: In some cases.

5 MR. GROMAN: In some cases. What is the relief
6 that you're looking for and what is your view on the
7 money judgments?

8 MS. SELIS: Well, this brings up a whole
9 question, how do you measure the injury? I mean there
10 are a lot of injuries with the receipt of Spam, some of
11 which are measurable and some of which are not. So, an
12 ISP who can say his system went down for two days and he
13 lost X amount of money has an easier time showing an
14 amount certain.

15 But a consumer who gets Spammed, you know, how
16 is he or she going to show that there is money actually
17 lost? So, our statute has a \$500 per Spam penalty
18 associated with it for consumers and \$1,000 per Spam
19 penalty associated with it for ISPs. Or, in the
20 alternative, if actual damages are more, then you can ask
21 the court to give you actual damages.

22 Your question, though, which I haven't really
23 answered, is how important are damages. I talked this
24 morning about deterrent effect, and I think that's -- I
25 have to come back to that. If you can hit a Spammer in

1 his or her pocketbook, then you've done a successful job.
2 Now, some of them are real mom-and-pop operations,
3 they're not making a lot of money, and so if you can hit
4 them with a \$10,000 judgment, that to them is a deterrent
5 and that will make them stop.

6 If, on the other hand, you come up against what
7 we'd call a Spam house, a really big operation, and I
8 don't think we have yet to take one of those down,
9 although I think we would like to, I would look to
10 getting a significant amount of damages. So, I think
11 damages are important, as long as they act as a deterrent
12 effect.

13 MR. GROMAN: Okay, following up on the same
14 path of the issue of the judgment, turning to my right,
15 there's certainly a big difference between filing a case
16 and getting a judgment, possibly by default and actually
17 collecting on that judgment, meaning -- and if you're not
18 collecting, are you really hurting someone in their
19 pocketbook. Starting with, Dietrich, have you had the
20 case where you've got judgments that are just not going
21 to be collected?

22 MR. BIEMILLER: We've got one right now that is
23 a Spammer down in Florida that we got a \$270,000 judgment
24 on that we're never probably going to see. The ones that
25 we have collected money are usually ones that have

1 settled. They see the writing on the wall typically and
2 will talk to us about, you know, getting out of it.

3 MR. GROMAN: Pete, you had -- the ISP cases
4 tend to make really fantastic headlines that read
5 something like \$25 million judgment against Smith on
6 behalf of Earthlink. Will you ever see that \$25 million?
7 I mean, has that been collected and what will happen with
8 that?

9 MR. WELLBORN: We're currently looking for that
10 off-shore as we speak. Will we get the whole \$25
11 million? Who knows. Will that send a message to every
12 other Spammer in the country, that if you Spam you'll get
13 the financial death penalty? Yeah, that's going to send
14 that message. And what's more, talking about the
15 remedies, it's just as important as the money, turning
16 back to the idea of injunctive relief, one thing that
17 we've done for the past three or four years for, you
18 know, for Earthlink in every case they resolve; for some
19 of the smaller ISPs as well that I represent, when we get
20 relief in these cases, we don't ask the court protect
21 Earthlink from -- Earthlink and Earthlink only from the
22 Spammer's future bad acts or if it's for Friendly E-mail
23 protect Friendly E-mail, no more bad acts against
24 Friendly E-mail.

25 Instead, we get an order from the court that

1 directs the Spammer never to Spam, spoof or commit any
2 other of a various list of prohibited conduct against
3 anyone in the world. And, in fact, the order makes all
4 ISPs and internet users worldwide express third-party
5 beneficiaries who can sue under that -- for a violation
6 of that order as if it were a contract to which they were
7 a party.

8 MR. GROMAN: Pete, do you think that the
9 Spammers you see are actually complying with that
10 injunctive relief?

11 MR. WELLBORN: I do, because among other
12 aspects of the relief, this is already the law, but we
13 stress it in all caps and bold face that violation of
14 this order will not only be a future Spamming violation
15 but will result in civil and criminal sanctions against
16 these Spammers. So, if you're talking about a small
17 amount of money or even a big judgment if they're poor,
18 maybe that doesn't get their attention, but if they
19 understand, and I've had judges look the defendants in
20 the face and tell them, if you violate this, you will go
21 to jail. And that gets people's attention.

22 MR. GROMAN: Do you -- I understand that you
23 say you believe they're following, but do you do what I
24 would call compliance monitoring? Do you have any actual
25 anecdotal or otherwise evidence that the Spammers aren't

1 just starting over under a different name in a different
2 state or location?

3 MR. WELLBORN: We do. There is one Spammer who
4 has -- he backslid, unfortunately, he Spammed me
5 personally.

6 (Laughter).

7 MR. WELLBORN: And this was a guy who got drunk
8 and told the -- got drunk, left a voicemail on my
9 client's voicemail saying that he was in cahoots with me
10 to Spam the client and have the client pay me legal fees
11 and that I would split my fees with the Spammer. And of
12 course when I played that tape for the federal chief
13 judge in Atlanta, Orinda Evans, and she just about had a
14 fit. She was not happy with this particular defendant.

15 But he Spammed me about six months ago, three
16 months ago, and I'm finishing up the -- my personal suit
17 to enforce the order of permanent injunction that we got
18 against him on behalf of a couple of smaller ISPs three
19 years ago. So, some backslide. Others that I've checked
20 on periodically, just knowing they were going to
21 backslide, have not.

22 So, yes, this global relief, it's really
23 important because it protects -- it keeps the Spammer
24 from moving on to smaller ISPs or smaller entities that
25 are less able to defend themselves than the Earthlinks

1 and the AOLs and the Microsofts of the world, and this is
2 something we all should use. I mean, I'll be happy, if
3 anyone in this room is a Spam plaintiff and you want to
4 e-mail me, I will send you the legal brief that explains
5 why that relief is appropriate and explains to the court
6 that the legal basis for awarding that universal relief,
7 even if the plaintiff is only a single company. I'll
8 give you my e-mail afterwards, and I will send that to
9 you the day you e-mail me.

10 MR. GROMAN: Okay, Jon, we'll give you the last
11 word on this idea. First of all, judgments, are the big
12 headline judgments that aren't collected, is that still a
13 deterrent? And then second of all, is this injunctive
14 relief doing anything?

15 MR. PRAED: Yes, to both. Press is obviously
16 an important part of what we're all doing, trying to get
17 the message out there. Judgments are the first step.
18 The first step is really before that. The first step is
19 making Spammers realize that every step of the way
20 there's going to be an increased cost to the business.
21 They operate typically on fairly thin margins. Those
22 that are making a great deal of money are working very
23 hard to try to do everything they can to hide. And if
24 you can get a judgment against them, even if it's not
25 collectible today, that's not to say it's not going to be

1 collectible tomorrow, and it's very difficult for
2 Spammers in my experience to discharge Spam judgments in
3 bankruptcy. That's a message that I think too few
4 Spammers realize.

5 But at the end of most of the cases that I have
6 been involved in, the Spammer has been quite upset by the
7 path that they have put themselves on. They understand
8 that they've -- I wouldn't say ruined their lives, but
9 they have made some tremendous mistakes along the way.
10 Even if they can't write a large check at the end, they
11 realize they're never going to be in a position to write
12 themselves a large check for a very long time.

13 And that has an effect on them and it obviously
14 has an effect. In fact, if this is a game of Whack-a-
15 Mole, your focus is largely on general deterrents and not
16 specific deterrents. And I think anyone who's thinking
17 of getting into the Spam game needs to think twice when
18 they see that many of the major players who are involved
19 in the internet space are committing significant
20 resources less towards recouping their costs of
21 litigation but rather towards generally reducing their
22 cost of hardware investment and of increasing the cost on
23 the Spammer.

24 MR. GROMAN: Okay, thank you. Let's turn back
25 to the idea of a private right of action, which had a lot

1 of attention this morning on the legislation panel.
2 There are those who believe that giving individuals who
3 receive Spam a private right of action to sue will have
4 an enormous deterrent effect.

5 So, Dietrich, I'll turn to you on this. First
6 of all, who are your clients and what are these lawsuits
7 about?

8 MR. BIEMILLER: Most of them are tech-savvy ISP
9 or tech people. I do have a small ISP. I've got a
10 landscape design engineering company that got relay-
11 raped. So, it's mostly -- I mean, I don't do any
12 advertising, it's mostly word of mouth and people hearing
13 about it through either media or friends.

14 MR. GROMAN: Are you litigating these Spam
15 cases full-time?

16 MR. BIEMILLER: Yes. Well, yeah, among my
17 other practice, but I'd say the majority of my stuff
18 right now is Spam cases.

19 MR. GROMAN: And how do these private right of
20 actions get resolved? Are these judgments, default
21 judgments, settlements?

22 MR. BIEMILLER: All across the gamut. We do
23 settle; we do default judgments. I haven't actually had
24 one go to court yet because we just started doing these
25 like last July and the court dates aren't, you know, that

1 speedy as we all know, but we're progressing through
2 discovery on most of these right now.

3 MR. GROMAN: I'm going to ask you a question
4 that I know that a lot of other attorneys have been
5 wondering. Does this make financial sense for you? Are
6 you making --

7 MR. BIEMILLER: I'm certainly not making money
8 like I would like to, as if I had a large-firm job. The
9 big payout at the end is quite the carrot though, if we
10 do get a large judgment against somebody who actually has
11 money and who actually pays it, which is three pretty
12 attenuated things. But the settlements are kind of
13 providing a war chest to go file more cases and proceed
14 with the ones that are in the middle.

15 MR. GROMAN: Who's covering the cost of these
16 private right of action cases?

17 MR. BIEMILLER: Right now, the co-counsel I
18 have, Mr. D. Michael Tompkins, who I rent space from, is
19 fronting most of these, but there really aren't that many
20 costs. I mean, we try to do it on --

21 MR. GROMAN: So, it's not the client, then?

22 MR. BIEMILLER: No, no. We haven't had that
23 many costs. Mostly it's just filing fees and that sort
24 of thing. We haven't done a lot of traveling and that
25 sort of thing.

1 MR. GROMAN: What is the goal of private right
2 of action cases?

3 MR. BIEMILLER: Well, the goal of the client is
4 to get the Spam to stop to them individually. And part
5 of every settlement that we've had we do get the
6 injunctive provisions, kind of like Pete was talking
7 about, and it works for them. I mean, we obviously don't
8 have the power to extend that -- well, I guess maybe we
9 do. I'd like to get that brief from you, Pete.

10 **(Laughter).**

11 MR. BIEMILLER: I might be trying to get that
12 incorporated, as well. But so far it's done a good job
13 for them individually, but we do have the Whack-a-Mole
14 situation, but if we want to go back to the analogy
15 earlier today, the viral thing, I mean, if we whack one
16 mole, if we just stop whacking them we're going to be
17 overrun with moles. So, you just have to keep whacking
18 until the problem changes.

19 MR. GROMAN: Why does an individual who wants
20 to file a right of action or a small company, under the
21 statute, need a lawyer? Shouldn't they be able to --

22 MR. BIEMILLER: Yes, we do have small claims in
23 district court that they can go to. The ones that come
24 to me, though, are typically large volumes. Like some of
25 my clients have 300 or 400 Spams that they want to deal

1 with from real prolific Spammers. And those -- they tend
2 to get in over their heads when they start getting
3 removed to federal court and that kind of thing.

4 But one of my other cases is a guy who won in
5 small claims court and they've appealed that all the way
6 up to the court of appeals at this point, to keep the
7 precedent from getting set. I guess the Spammers
8 appealed it.

9 MR. GROMAN: Okay, I'd like to raise the issue
10 of abuse litigation. And since you are the member of the
11 plaintiff's bar on our panel, I'm going to toss it at
12 you.

13 MR. BIEMILLER: Okay.

14 MR. GROMAN: There are those who would
15 articulate a view that Spam statutes are going to be
16 abused by the plaintiff's bar and that it might as well
17 just be a personal injury case, it really doesn't matter.
18 They're going to find a statute and they're going to
19 abuse it as a money-making scheme. And is that a
20 legitimate concern and does it matter?

21 MR. BIEMILLER: Well, I guess we've heard all
22 about Utah this morning. We don't have that problem
23 here. I guess like any kind of litigation it can be
24 abused, so it's really going to be an individual case
25 type thing. I don't feel like I'm abusing it personally.

1 It's just like a personal injury thing; you have to have
2 a car wreck to bring a suit on that. With us, it just
3 seems overwhelming because we have a bazillion million
4 car wrecks to deal with. So, if that means we're suing
5 to enforce a lawful statute to try to stem the tide of
6 this stuff, I can't see that as abusive.

7 Further, it's kind of ironic that those who
8 talk the most about we're trying to make money off this
9 are the Spammers themselves who by their very definition,
10 that's what they're doing when they're Spamming, is just
11 trying to make as much money as they can, so --

12 MR. GROMAN: I want to open up that same
13 question to Jon and Pete and just see if you have
14 anything to say about this concern that Spam statutes and
15 Spam litigation might actually have a chilling effect on
16 legitimate companies who are fearful of litigation. You
17 don't have to take it, but --

18 MR. PRAED: I think as Dietrich suggested,
19 abuse is not unique to Spam litigation, and the concept
20 of abuse and the mechanisms to prevent it have been
21 around for a long time. Rule 11 is as effective in Spam
22 litigation as it is anywhere else. And I think that
23 those deterrent powers are perfectly adequate to keep
24 people from using Spam litigation abusively.

25 I quite frankly think, though, if you're

1 talking bottom line justice that I have seen far more
2 abuse on the defense bar in Spam cases where you have a
3 defendant who is engaging in fraudulent Spam. There have
4 been -- I don't want to talk about particular cases, but
5 it is not unusual for Spammers to literally throw their
6 computers away in order to keep them from being
7 discovered. It's not unusual for -- I think one could
8 argue that many of the answers that are filed in response
9 to complaints are dancing on the line of Rule 11.

10 Those are abusive tactics, as well, and are as
11 worthy of concern in an age when you can debate what "is"
12 means. I think it is a real risk to fall into the trap
13 that Spammers think that litigation over Spam is a
14 continuation of the game that is Spam. And I think
15 they're learning -- you know, Virginia has just -- or has
16 just enhanced its criminal statutes. I think the day has
17 come when Spammers are going to realize this is not a
18 game. And likewise, people who engage in abusive conduct
19 on the plaintiff's side, there are adequate measures in
20 place to prevent that.

21 MR. GROMAN: Thank you. I'm going to turn back
22 to my colleagues in the state government. Eileen asked a
23 question this morning on the legislation panel that I
24 thought was from my panel, but she's my boss, she can do
25 that. And it was to Paula, so I'm going to turn the

1 exact same question to Stephen.

2 Twenty-nine states have Spam statutes, and I
3 believe we've only see action out of three states. Why?

4 MR. KLINE: Well, I can tell General Spitzer
5 will kill me if I start guessing as to why other states
6 are not acting. I can tell you why -- it's tough. I
7 mean, you're looking at our Spam litigation team. It's
8 me and my civilian investigator. And it's not even full-
9 time. I've got, you know, ten other cases that I handle
10 as well.

11 MR. GROMAN: And that's for the State of New
12 York which is a comparatively big state.

13 MR. KLINE: That's for the State of New York,
14 yeah. And so there are -- I think one thing that you see
15 in both the criminal side in which I've had experience
16 and in this side is that a lot of the states attorneys
17 just don't have the training in high-tech cases. It's
18 expensive. It's -- once people get training in that
19 area, it's -- there are certainly a lot of lucrative
20 offers that come along. And, so, I think it's, one,
21 tough to find people who can do it; two, I think it's
22 tough to find the money to do it. And I think in some
23 situations it may be tough to find the higher-ups that
24 understand what's going on or understand the seriousness
25 of it.

1 MR. GROMAN: Paula, how many --

2 UNIDENTIFIED SPEAKER: Can you elaborate on
3 those lucrative offers?

4 **(Laughter).**

5 UNIDENTIFIED SPEAKER: A little more on those,
6 please.

7 **(Laughter).**

8 MR. GROMAN: Paula, how many attorneys with the
9 Washington State AG's Office are working on Spam issues?

10 MS. SELIS: You're looking at the one. I am
11 she. I agree with Stephen, everything that he said is
12 true. And just to highlight that, Spam is, I think
13 everybody in this room recognizes, it's a problem, and
14 it's a huge economic problem. But when you have
15 consumers who are calling you about the fact that they
16 have lost \$10,000 to a telemarketer and you've got to
17 decide whether you're going to help that consumer or
18 whether you're going to file a Spam suit where nobody's
19 really lost any money, although the entire internet
20 community has lost a significant amount, oftentimes
21 you're going to take the case involving the telemarketer.
22 And those are very real pressures, priorities that state
23 AGs face every day. So, you know, I don't want to malign
24 our brethren, sistren in other states, but there are good
25 reasons for not taking Spam cases.

1 MR. GROMAN: I was going to follow up on that,
2 but I'm actually going to turn that same question to the
3 counsel for the big ISPs and say that there are those who
4 would say that your -- the companies represented actually
5 brought relatively few Spam cases. I think Earthlink's
6 about a dozen. I think in total, from the press release
7 I read about AOL, it's 25 total. And between May of 2001
8 and April of 2003, they brought no cases. So, why do you
9 think that would be?

10 MR. PRAED: Well, I don't know that those
11 numbers are necessarily correct, and I don't want to
12 debate the numbers with you necessarily. I will say
13 bringing a lawsuit, first of all, is a tremendous
14 commitment of resources. And there have been, I think, a
15 lot of lawsuits brought, but the bringing of a lawsuit is
16 really the tip of the iceberg. I think you're seeing the
17 state attorneys general bring relatively few cases
18 because it is so resource-intensive. It's resource-
19 intensive for the ISPs, as well, regardless of size.
20 And, again, it's a game of Whack-a-Mole. I think there
21 are tremendous, tremendous volume of resources being
22 devoted, first of all, to maintaining the networks. I am
23 amazed at the job that large ISPs and small ISPs are
24 capable of doing.

25 I would challenge -- I think it's remarkable in

1 a sense to step back and identify any other business
2 enterprise that is capable of withstanding essentially 40
3 to 70 percent free ridership problem. The Metro system
4 here in town would collapse if 40 to 70 percent of us
5 were jumping the turnstiles. There is no other business
6 today that could support that level of free ridership,
7 but it is not free in the end for the ISPs.

8 And what they are doing both in terms of
9 managing the daily volume that they have and
10 systematizing the investigation that allows them to put
11 in place a process that culminates in a lawsuit. It is
12 one thing to issue 14 subpoenas. Issuing subpoenas is
13 really the last step in the process of sending letters,
14 making phone calls, doing some very thorough
15 investigations that provide you a great deal of
16 information and that have real repercussions.

17 I'm as proud of the fact that we oftentimes
18 chase Spammers across the network space as I am over the
19 fact that we may sue them and identify them. Don't
20 misunderstand. We put costs on Spammers the day we start
21 thinking about them, not the day we start suing them.
22 And that's the trick, is to try to find ways -- I want
23 them in this room. We're all in a sense wasting our time
24 talking about the problem. We need to go sit at
25 computers and do the very hard work that the major ISPs

1 and the government officials and the solo practitioners
2 are doing.

3 MR. GROMAN: I have a question to follow up on
4 you, and I'd like a quick answer on this one. Do you
5 subscribe to the point of view that there really are 150
6 big guys out there doing most of the Spamming?

7 MR. PRAED: I don't know that that number's
8 right, but I think you'd be shocked by how many few very
9 big fish there are.

10 MR. GROMAN: Pete, do you agree with that?

11 MR. WELLBORN: I do right now, but what's scary
12 is that going back to a theme of technology one-
13 upmanship, if you go back to the Sanford Wallace days,
14 you had to be an internet rocket scientist to figure how
15 to pop these e-mails out, and even then you're doing it
16 at a rate of thousands a day. Nowadays you've got script
17 kiddies, you've got people who can barely log on that
18 download this software, follow the idiot-proof directions
19 and those people are popping out a million e-mails a day.
20 And when you do the math, it's staggering, not even look
21 at a honed reputation.

22 MR. GROMAN: So, is that a way of saying
23 probably not just 150 people?

24 **(Laughter).**

25 MR. WELLBORN: I'm saying right now possibly

1 yes, but if we don't do something, it's going to be --
2 that the number of awful, awful Spammers is going to
3 grow.

4 **(Applause).**

5 MR. GROMAN: Okay. So, while we're on the
6 topic of big ISPs, we've heard that -- it happened on --
7 this Monday, AOL, Yahoo and Microsoft announced that
8 they're going to have increased coordinated efforts with
9 law enforcement to enhance enforcement efforts against
10 Spammers. My question to Paula and Stephen is what is it
11 that you want to see AOL, Yahoo and Microsoft do to help
12 both of you do your jobs.

13 MS. SELIS: Well, having had some experience in
14 our own backyard with Microsoft and some very good
15 cooperation, I'd like to see them and other ISPs take
16 action and sue more Spammers. I think that would be a
17 huge step and a step in the right direction. Also,
18 information sharing, at least in Washington we have a
19 data base of Spam complaints, sort of a mini FTC data
20 base from Washington residents. And we would share that
21 information with the ISPs so that they could use it to
22 target Spammers. In turn, if there were a case or a
23 particular Spammer who they thought would be best served
24 by a state lawsuit, we would like to be able to take
25 that. So, I think there is a lot of room for

1 cooperation.

2 MR. GROMAN: Stephen?

3 MR. KLINE: I haven't run into any problems
4 with the three of them. I think the intelligence-
5 sharing, which we've started, has been unbelievably
6 helpful. And, you know, every time our name winds up in
7 the paper for a MonsterHut or something, we always wind
8 up with 20 phone calls, some of them anonymous, some not
9 so anonymous, saying well, there's five other Spammers,
10 and here's some information.

11 You know, I would encourage not just the big
12 ISPs, but the smaller ISPs, and any other sys-admin out
13 there who has information on this, to pick up the phone
14 and call your local AG. And if your local AG doesn't
15 seem that up on the issues, sit down and educate them,
16 you know? You know, we're not going to know as much as a
17 sys-admin, but we're happy to be educated about it. And
18 that's where the good cases are going to come from.

19 MR. GROMAN: We followed the international
20 panel, and in my conversations with all of you before
21 this panel, you all mentioned that you encounter concerns
22 and challenges in the international arena. So, what are
23 the issues as litigators that you're facing in terms of
24 international issues. I'll start with you, Pete.

25 MR. WELLBORN: I knew you were going to start

1 with me, because I told you just to skip me on that
2 question before we started that panel.

3 **(Laughter).**

4 MR. WELLBORN: And I'll speak very honestly.
5 When an international issue is figured in, that can make
6 the case and the discovery and the investigation a
7 horrible pain in the rear. The best thing to do, it goes
8 back to what we said earlier, which is follow the money,
9 because if you have a Spammer from whatever-stan, chances
10 are that Spam is not asking you to mail your check to
11 some small town in whatever-stan. Instead, that's either
12 a third-party relay, where the operation truly is in the
13 U.S. or if it's especially sophisticated, it's a foreign
14 mailer for a U.S. company. So, the first thing I do when
15 I see any kind of indicia of foreign involvement is
16 redouble my efforts to follow the money, and nine times
17 out of ten, if not higher, I'll confirm that, hey, that
18 was just a smoke screen, this is a guy down in Florida,
19 or this is a guy up in New York.

20 MR. GROMAN: Would you be less inclined to file
21 a case if you know there's a large international
22 component?

23 MR. WELLBORN: I would not be less inclined,
24 but I would steel myself for the battle.

25 MR. GROMAN: Jon?

1 MR. PRAED: International is a major problem,
2 and it's a growing problem. But, again, it's not a
3 problem that's unique to Spam. I don't think it should
4 deter Spam litigation, but you do have to plan for it.
5 And one large thought, obviously there needs to be
6 coordination, international coordination, and I know that
7 that's happening, in large part with the FTC's help. And
8 I applaud that, that international coordination.

9 I think, though, there's a technological
10 coordination, as well, which involves providing the
11 individual consumer the ability to tell their browser or
12 their mail service that they want to respect geo-
13 political boundaries and literally tell their browser I
14 do not want you to take me to websites that are hosted in
15 the former Soviet states. Right now, that is not
16 technologically possible very easily, certainly not by
17 the average consumer, and it's something that the
18 consumer, I think, would applaud being provided that sort
19 of empowerment.

20 MR. GROMAN: Dietrich, anything on the
21 international front in your cases?

22 MR. BIEMILLER: We tend to figure that into the
23 low-hanging fruit analysis and avoid them when possible.

24 MR. GROMAN: Paula?

25 MS. SELIS: I'll have to echo Dietrich on that.

1 It's very difficult using state resources to handle a
2 foreign aspect to a case.

3 MR. GROMAN: Stephen?

4 MR. KLINE: I would have to echo that, as well.
5 We did have a foreign aspect in the MonsterHut case, Gary
6 Hartle, the technician that we sued was living in Canada,
7 I think did most of his work from Canada, his non-
8 MonsterHut work. When he heard -- we got a little lucky
9 with a dumb defendant, because when he heard that we were
10 looking for him, he called us and --

11 MR. GROMAN: That makes it easy.

12 MR. KLINE: -- asked us if he could -- if we
13 could go to his attorney's office in Niagara Falls to
14 serve him in front of his attorney, rather than coming up
15 to Canada, and we said of course you can come back to the
16 U.S.

17 **(Laughter).**

18 MR. KLINE: You know, I'm not so scared of the
19 international aspect anymore, I guess.

20 **(Laughter).**

21 MR. KLINE: But generally, yeah, it -- the
22 second we see it go to another country, the process for
23 us is such a laborious one and such a time-consuming one
24 that we really have to consider whether that's the best
25 use of our resources.

1 MR. PRAED: Marc, if I can, I'd -- anyone who
2 wants a good primer on how complex the international
3 arena can be, AOL in the CN Productions case moved for
4 contempt against the defendants after having gotten a
5 judgment against them. They continued to send Spam, and
6 we brought a motion for contempt and were ultimately
7 successful in that. AOL on its legal website has a
8 lengthy brief that explains the factual scenario behind
9 what was an international conspiracy. And I think the
10 facts would be -- it's a fascinating reading for people
11 who are really interested in that aspect of the Spam
12 fight.

13 MR. GROMAN: My last question for each of you,
14 before I open this up to the audience, is what is the
15 greatest challenge ahead, the greatest practical
16 challenge ahead, in terms of Spam litigation? Stephen?

17 MR. KLINE: Manpower. It is tough trying to
18 justify spending so much time and energy on a case where
19 we're not getting any money back to consumers and the
20 money for penalties isn't there and, you know, we get an
21 injunction and they flee the country. So, it's --

22 MR. GROMAN: Resources.

23 MR. KLINE: Yeah, resources really is just the
24 toughest part.

25 MR. GROMAN: Paula?

1 MS. SELIS: I'd have to agree with that. I
2 think resources and I think that the potential challenge
3 is bad Federal law, I'm hoping that we don't face that.
4 But given our current status, I think the biggest
5 challenge is resources, the technical savvy, the people
6 and the money to actually take these cases forward and
7 win and to make it justifiable in the end.

8 MR. GROMAN: Dietrich, your thoughts?

9 MR. BIEMILLER: I can pretty much echo both of
10 those things, even just from a small private side, trying
11 to match up the resources and then the collections end on
12 the other end. That's going to be a tough connect on
13 some of these cases.

14 MR. GROMAN: Jon?

15 MR. PRAED: I'd echo that. Resources, and I
16 think on a longer term, eventually the real hard-core
17 fraud-Spam problem is going to be solved, I think, in the
18 next couple of years. Then we'll be left with a low-
19 level threshold of Spam, largely coming from young
20 teenage boys. And I think our challenge as a nation, to
21 be honest, is to find some way to engage some very sharp,
22 young people, so that they can be challenged in a way
23 that is fruitful. And dealing with that and finding a
24 way to collectively do it, I think, is quite honestly our
25 biggest challenge.

1 MR. GROMAN: Pete, you get the last word.

2 MR. WELLBORN: I think the biggest challenge is
3 to generally deter the number of Spammers, because the
4 technology, as it increases, puts so much power to do bad
5 in the hands of so many people who don't have to be
6 rocket scientists. We talked about a Whack-a-Mole idea,
7 we need to take some Whack-a-Moles, and after we whack
8 them, draw them, quarter them, put their head on a spike
9 and parade that in front of the other Spammers.

10 **(Laughter).**

11 MR. WELLBORN: We really do need to send a
12 message.

13 **(Applause).**

14 MR. GROMAN: On that colorful note, would
15 anyone care to ask any of these trial attorneys
16 questions? Where are the microphones? Okay, right up
17 here in the front, the gentleman on the end. Please
18 identify yourself and wait for the microphone.

19 MR. TYNAN: Dan Tynan, PC World Magazine. You
20 guys have talked about Spammers engaging in fraud, in
21 forgery, in hiding money off-shore, pump-and-dump
22 schemes, a lot of pretty serious criminal activities.
23 Have any of you in your investigations uncovered links to
24 organized crime, and if so, would the RICO statutes
25 apply?

1 MR. GROMAN: Why don't we start with the AGs.

2 MS. SELIS: No.

3 **(Laughter).**

4 MS. SELIS: New York is bigger; you go first.

5 MR. KLINE: You know, we've only had one case
6 publicly, and anything that's pending, we couldn't
7 confirm or deny. But I wouldn't be surprised if you
8 started seeing money pop up in places like that.

9 MS. SELIS: Ooh.

10 **(Laughter).**

11 MS. SELIS: Well, we have not thus far seen any
12 links with organized crime, but you bring up something,
13 which is that apart from the Spam we oftentimes see an
14 underlying scheme that we find problematic, you know, a
15 get-rich-quick scheme or a wonder drug or something like
16 that. And when we bring our cases, we not only file
17 against them for purposes of violating our Spam statute,
18 but we also allege that they're violating our consumer
19 protection act by making misrepresentations, which isn't
20 quite a crime, but it's a sort of similar kind of
21 activity.

22 MR. KLINE: You know, I think there's one
23 similar example. I think any time that there is an easy
24 way, a shady way, to make money, organized crime is going
25 to start to find their way into it. A perfect example of

1 that is a case I handled with the FTC against Crescent
2 Publishing. We -- there was \$300 million worth of credit
3 card fraud for -- through adult websites just -- I want
4 to say a month ago, a month and a half ago. The Eastern
5 District of New York and the U.S. Attorney's Office in
6 the Eastern District of New York indicted Bruce Chew and
7 two others involved for laundering money and kicking back
8 about \$8 million to the Gambino family, was it? Yeah.

9 MR. GROMAN: Next question. The lady over here
10 with the glasses, please.

11 MS. BECKER: Francois Becker from L-Soft
12 International. If you're a legitimate list operator with
13 double opt-in and everything, what kind of information do
14 you need to keep on each of your subscriptions to protect
15 yourself from frivolous lawsuits by people who subscribe
16 and then claim you Spammed them?

17 MR. GROMAN: Do you want to pick a lawyer to
18 answer that? Anyone want to handle that one?

19 MR. WELLBORN: I'll take it. The most obvious
20 information in relation to the three-way handshake that
21 you allude to, which is a means of confirming someone's
22 opt-in, it's to keep false opt-ins -- if I wanted to
23 really get back at one of ya'll, I could go to all these
24 different sites and opt-in your e-mail address and then
25 suddenly you're getting flooded with Spam.

1 To prevent those false opt-ins, there's
2 something called a three-way handshake where the list or
3 the mailer to whom that e-mail address is opted does not
4 just start Spamming, an e-mail is then sent to that
5 person that says someone opted you in, we think this was
6 you, if you do not reply to this, you'll never hear from
7 us again. If it really was you, reply back. And, so,
8 you actually have the reply coming from the e-mail
9 address that was opted in. So, I'd say first and
10 foremost, keep all information available, logs,
11 everything, about each aspect of that three-way
12 handshake.

13 MS. BECKER: But you've got millions --

14 MR. GROMAN: Do you need a microphone?

15 MS. BECKER: If you have millions of
16 subscribers throughout many lists -- if you have millions
17 of subscribers, you're still saying we need to keep every
18 single e-mail, or is it enough to have the IP address
19 that the okay came from?

20 MR. WELLBORN: I would keep

21 AUDIENCE MEMBER: (Inaudible) -- I mean,
22 there's a cost to doing business.

23 MR. WELLBORN: I would say definitely keep
24 every bit of the transaction, because especially -- my
25 radar goes up, when people start talking about opt-in

1 lists with millions of people --

2 MS. BECKER: We've got hundreds of thousands of
3 lists, each of them -- I run an epilepsy support list,
4 500 people. We've got a site that has --

5 MR. GROMAN: Keep the follow-up very short,
6 please.

7 MS. BECKER: We've got 200 cancer lists.
8 There's a lot of people with cancer, and there are cancer
9 support people. And we've got volunteers operating
10 these. We don't have -- this isn't necessarily a money-
11 making thing for some of them.

12 MR. WELLBORN: With the cost of storage, save
13 all you can and you also have an important factor, a
14 different conversation for a different time. I'm not
15 sure you all are commercial, based on what you just said
16 right now, so the rules are a little bit different for
17 non-commercial activities.

18 MR. GROMAN: Okay, we'll move to the next
19 question. Do we have any questions from the internet?
20 Okay, any other questions from the audience here? Can we
21 have the gentleman over here, please? Please identify
22 yourself.

23 MR. GELLER: Hi, my name is Tom Geller from
24 Spamcon Foundation. And my question is for all of the
25 attorneys, especially the trial attorneys. How do you

1 manage consumer demand for your services? At Spamcon
2 Foundation, we don't actually address individual Spam
3 issues, but it doesn't stop dozens and dozens of people
4 every week writing to us saying I received this Spam, can
5 you help me out, can you figure this out for me. And I'm
6 just assuming that it's similar for you folks.

7 MR. GROMAN: Paula, what do you do? You must
8 get thousands and thousands of e-mails in your data base,
9 consumer complaints. What do you do with them and how do
10 you pick the case?

11 MS. SELIS: Okay, good question, good question.

12 MR. GROMAN: And I hope I paraphrased that okay
13 for you.

14 MS. SELIS: A good example, just recently,
15 there were 1,700 complaints during February of this year,
16 so that gives you kind of an idea of the volume. And
17 we're very lucky, we have a website that we put a lot of
18 consumer education material on, tell people how to file
19 their own private actions if they want to. But we can't
20 handle each and every one individually; we can't file a
21 lawsuit on behalf of them all.

22 So, what we do is we give them the consumer
23 education materials. We have them file a complaint on-
24 line, which enables them to cut and paste their Spam
25 complaint onto the computer itself, and we keep a data

1 base of that. And then we periodically look at what's in
2 our data base, having already given the consumer his or
3 her education and decide, based on what we find, what
4 would be a good case for us to bring.

5 MR. GROMAN: Does anyone else want to field
6 that question?

7 Okay, let's move on. In the back, with the
8 Spam hat.

9 **(Laughter).**

10 MR. GROMAN: We had to go there, right?

11 MR. FERGUSON: Jim Ferguson, I'm not spews
12 (phonetic).

13 **(Laughter).**

14 MR. FERGUSON: What about the opposite side of
15 the house where the Spammers are suing the anti-Spammers
16 because we're denying them access to our personal
17 inboxes, as well as our networks?

18 MR. GROMAN: If someone would like to take
19 that, I'd like you to keep that brief. It's slightly off
20 topic --

21 MR. WELLBORN: I'll keep it real brief. To the
22 extent you're alluding to any particular case, since it's
23 a business entity that was formed just a couple of weeks
24 ago, two months ago, we don't know who it's composed of,
25 but if there's an entity that's composed of Spammers, and

1 by Spammers I mean people sending unsolicited commercial
2 e-mail into computer networks that they know forbid
3 unsolicited commercial e-mail, those people are
4 criminals, and for them to file suit is analogous to a
5 burglar suing you because you put a lock on your door.

6 (Laughter).

7 MR. GROMAN: The gentleman in the back by the
8 door, please.

9 MR. CROCKER: Hi, Dave Crocker, Brandenburg
10 Networking. First of all, I'd like to thank you all for
11 a great amount of candor, no matter how disconcerting it
12 might be. It helps bring some reality to the
13 expectations about legal enforcement of all this. And
14 that ended up highlighting two disparities that I'd like
15 to pursue. One I want to highlight and one I want to ask
16 about.

17 The one I want to highlight is the comment
18 about geographic boundaries and any expectation that
19 we're going to be able to tell browsers, oh, just don't
20 go to that country. And it was said that it's not
21 something you could do now. I will tell you, I don't
22 know how to do that, and I ought to, and I don't know how
23 to do that. So, I think that any expectation that
24 browsers are going to be able to do that any time in the
25 near future, like 10 or 15 years, is pretty small.

1 The other disconcerting -- or disconnect that
2 I'd like to ask about and get some feedback on is we have
3 for most of this workshop been hearing about the high
4 expectations that are held for passing laws and having a
5 strong effect on Spam. And I would say that your
6 consensus sounds an awful lot like that ain't going to
7 happen, and would like you to speak to that some, please.

8 MR. GROMAN: Do you want to pick somebody? Who
9 wants to field it?

10 MR. PRAED: I don't want to field that portion
11 of the question, but I want to field -- we've been to the
12 moon. We can certainly teach internet browsers how not
13 to go to former Soviet states or to the Bahamians, the
14 Bahamian Islands.

15 MR. GROMAN: Okay, the part of the question
16 about is this legislation really going to do anything?
17 Or are we kidding ourselves?

18 MR. CROCKER: My background's technical. When
19 I said this, we haven't taught anybody how to stop war.
20 There are lots of things we can't do. There are physical
21 limits in this world.

22 MR. GROMAN: Okay, I want to stick to the issue
23 of litigation and legislation, off the browser topic.
24 Anyone want to give an opinion, as a litigator, if we
25 have legislation that wants or seeks to encourage

1 litigation or law enforcement, are we going to see
2 anything happen?

3 MR. WELLBORN: As far as the legislative end of
4 things, if we have a law that tightens the noose, I'm all
5 for that. If we have a law that arguably or purports to
6 legalize that which is illegal right now, I'm against
7 that, and in fact, it would be a bad Constitutional
8 problem because an ISP's right to regulate how its
9 computers are used, that's one stick in its bundle of
10 property rights.

11 And, so, if you have any situation where the
12 government comes in and says, ISP, you can no longer sue
13 under common law trespass, you can no longer say that
14 people can't send unsolicited commercial e-mail through
15 your network, if that were to happen, there'd be serious
16 Constitutional issues. Right now, even without the Spam-
17 specific laws, which we would all love one if it had
18 teeth and it were good, but even without that, our gun's
19 already loaded with about a dozen or so bullets, any one
20 of which will get the Spammer.

21 MR. GROMAN: Okay, next question. Gentleman in
22 the back row.

23 MR. BERLIND: Hi, David Berlind with CNET. And
24 to Paul Wellborn's last point that drew quite a bit of
25 reaction from the audience, which is we should draw and

1 quarter Spammers, my question is, you know, we watched
2 the news recently, now that the war is over, the news is
3 going to other things, and one of the big focuses now is
4 how none of these people who have run afoul of good
5 corporate governance haven't gone to jail yet.

6 And the question here is, you know, I think a
7 lot of people believe that in the world of Spamming,
8 assets can be hidden and financial penalties are kind of
9 worthless, but if we make examples of a few people and
10 put them in jail that might change things, because you
11 can't hide the body. You can hide the money, but you
12 can't hide your own body, and so, what is it going to
13 take to improve the punishment from the recipient's point
14 of view to make a few examples here so that Spammers do
15 really think twice because the punishment is much more
16 serious than something that they can --

17 MR. GROMAN: Is the question do we need a
18 bigger punishment?

19 MR. BERLIN: Sure.

20 MR. GROMAN: Anyone want to field that?

21 MR. WELLBORN: I hate to take every question.
22 Make me prosecutor for a day, I'll put them all in jail.

23 **(Laughter).**

24 MR. GROMAN: Okay, we have a question up here,
25 please. Right up here in the front row.

1 MR. KELLY: Hi, Ben Kelly, Attorney in Los
2 Angeles. I have a quick question for probably mostly the
3 litigators here. What has been -- what are your thoughts
4 or what have your experiences been with a would-be Spam
5 plaintiff's duty to mitigate?

6 MR. PRAED: I'll take that. Obviously duty to
7 mitigate is a standard requirement. I think most of my
8 clients in my experience have fully discharged that duty
9 and are doing everything they can both to filter and to
10 put Spammers on notice. I think the Verizon Online
11 versus Ralsky case really stood for the principle that no
12 professional Spammer today can realistically say that
13 they don't know that what they're doing is in violation
14 of what Pete so eloquently points out is one of the most
15 important bundles in the bundles of sticks that we all
16 have, the right to exclude others from our private
17 property. Duty to mitigate is not a new concept.
18 Plaintiffs generally meet that duty fairly easily.

19 MR. GROMAN: I want to return to an earlier
20 question and give our former assistant district attorney
21 an opportunity to address that question about increased
22 penalties. Stephen:

23 MR. KLINE: You know, I agree with Pete that if
24 a few of them were in jail it would be tougher for them
25 to Spam. The problem that we have, and we have secondary

1 criminal jurisdiction in New York, is the same sort of
2 problem we have on the civil side, and that is, you know,
3 for all the resources we have, if I marched into my boss'
4 office and said you wouldn't believe this guy is sending
5 billions and billions of e-mails every day, and it's
6 costing this large corporation a lot of money, and on the
7 other side there's another assistant saying and over here
8 we've got people who are creating false passports for
9 terrorists, they're laundering money through Aholla's
10 back to Pakistan and all of this, I can tell you who's
11 leaving the office first and looking for another case.

12 **(Laughter).**

13 MR. KLINE: And I think Pete would agree.
14 We've talked about this a little. As much as we despise
15 Spammers, I'd much rather see a pedophile or a terrorist
16 taking up that jail space than a Spammer.

17 MR. WELLBORN: As would I.

18 MR. PRAED: Just a quick comment. I think,
19 though, what we're seeing is an exploitation of what in
20 the end is a systematic problem, and I think Spammers are
21 taking advantage of those same exploits that terrorists,
22 quite frankly, are taking advantage of. And to the
23 extent that we're -- to some sense and some degree it
24 doesn't matter who you chase, as long as you are chasing
25 someone who is taking advantage of that exploitation and

1 close the loophole. You're going to fix both problems.

2 MR. GROMAN: Okay, let's move on to another
3 question. The lady up front please, in the white.

4 MS. ANGWEN: Hi, Julia Angwen (phonetic) of the
5 Wall Street Journal. On the same note of increased
6 penalties, I'm just wondering why, if some of these
7 Spammers are using stolen credit cards and engaging in
8 fraudulent marketing, why hasn't there been any criminal
9 prosecution of them?

10 MS. SELIS: Well, I have to come back to what
11 Stephen was saying in terms of resources. There are a
12 lot of potential criminal cases out there, and when you
13 are facing, you know, property crimes versus physical
14 crimes versus terrorism and you have to choose among them
15 because you have limited resources, what oftentimes
16 happens is that you're going to go to the more serious
17 crimes first. And of course that's a philosophical
18 question as to what is the most serious one, but
19 oftentimes it's the one where there involved some sort of
20 bodily crime.

21 The Washington AG's Office does not have
22 criminal jurisdiction, but we do try to look at the
23 underlying issues. So, for example, if there is credit
24 card fraud or if there is a misrepresentation going on,
25 we may refer something out to the prosecutor. And there

1 is a question as to whether the prosecutor is going to
2 take it or not. I can speak in the off-line world, where
3 we have had just generic consumer protection cases that
4 have involved identity theft or fraud, and I have
5 referred some of those cases to our prosecutor and
6 sometimes the prosecutor will take them, if they involve
7 enough dollar loss, and sometimes our prosecutor will
8 not. So, it really comes down to resources once again.

9 MR. GROMAN: I also want to point out in
10 response to that question if you have a Spammer who is
11 engaged in Spam but is also engaged in identity theft or
12 credit card fraud or some other criminal behavior, that
13 individual may very well have been prosecuted criminally,
14 it's just not a Spam case necessarily. So, maybe they
15 did go to jail for the other behavior, but it wasn't a
16 Spam case under the Washington AG Spam statute.

17 So, I don't want to leave the idea that these
18 people aren't being prosecuted; they very well maybe,
19 it's just that it's not a Spam case then, it's a
20 different criminal action.

21 Yeah, I'll take a question from the gentleman
22 in the back, please.

23 AUDIENCE MEMBER: How do I go on notice saying
24 that I don't want Spam sent to my domains? I'm not an
25 ISP or anything. To whom do we send the check so that

1 the AGs can go to their bosses and say people are willing
2 to pay for this?

3 MR. GROMAN: The IRS.

4 **(Laughter).**

5 AUDIENCE MEMBER: But the IRS doesn't know that
6 I'm sending that check for this purpose. And can we
7 create automated tools that facilitate the tracing of who
8 it is that's sending the Spam so that it provides easier
9 ways for the AGs and attorneys to figure out who to go
10 after?

11 MR. GROMAN: The question's about automated
12 tracing.

13 AUDIENCE MEMBER: Yes, the question is is --
14 you know, can we create Spam bait out there like
15 honeypots are doing and things like that to try to go and
16 trace back who the Spammers are, so that the information
17 is gathered, held onto and traced back and tools for
18 figuring out --

19 MR. GROMAN: Well, I think that the next panel
20 actually is going to address some technical issues, so
21 let's keep this to litigation, and we'll leave that to
22 the next panel.

23 If we could have the gentleman in the back,
24 right behind you, please.

25 MR. SILVER: Hey, my name is David Silver.

1 Pete, I have a quick question for you just real quick.
2 You had made a comment to a lady's question earlier
3 about, you know, the kind of information that needs to be
4 kept in order to prove whether you've not done Spam or
5 not. So, just a point of clarification, so companies
6 that may be not practicing double opt-in, are they at
7 risk of being -- having a lawsuit filed against them?
8 Because I think this question of what attributes are
9 required to be kept is really important for lots of large
10 corporations that are trying to identify how do they
11 fight -- or keep from being sued as a result of what
12 attributes are required to be kept. And many companies
13 don't do double opt-in. So, I just have a question for
14 you, are they open to a lawsuit as a result of not having
15 that information?

16 MR. GROMAN: And you can send a bill for legal
17 services when you answer that.

18 MR. WELLBORN: Oh, that's a great question, and
19 it reminds me of an old contracts professor I had in law
20 school. He would say you can sue the bishop of Boston
21 for bastardy, but you might not win.

22 **(Laughter).**

23 MR. WELLBORN: And what that means is that
24 might you get sued? Yes, certainly. If someone falsely
25 opts in an e-mail address and there's no three-way

1 handshake to confirm that e-mail address, might that
2 person get mad and sue. Yeah. Would your client
3 possibly win because they had no way of knowing or they
4 weren't one of these outfits that's in the business of
5 taking false opt-ins, you know, yes, but the key factor
6 there -- I would advise one of my clients to not think
7 about what lets you win the lawsuit but instead think
8 about what lets you avoid the lawsuit altogether.

9 MR. GROMAN: Next question? We're going to go
10 all the way into the back corner. And please identify
11 yourself before your question.

12 MR. LEVINE: I'm John Levine from CAUCE Abuse
13 Net, and I have sort of a question and a half about
14 private right of action.

15 MR. GROMAN: Well, we're almost out of time, so
16 if we can keep it quick, please.

17 MR. LEVINE: The junk fax law is primarily
18 enforced by private right of action. Two things to make
19 it hard is it's complicated to explain to small claims
20 judges who frequently don't have a lot of real training,
21 and the other is that small claims have to be filed in
22 the defendant's location, which with faxes is frequently
23 the same as yours but with Spam never is. I'm wondering,
24 is there anything we could do to make PROA more
25 enforceable for small plaintiffs who have received Spam.

1 MR. GROMAN: Dietrich, that would be you,
2 private right of action.

3 MR. BIEMILLER: Well, I think the
4 jurisdictional issue is one -- I've got one case right
5 now that was brought in small claims court and the
6 defendant appeared over the phone, so it's really not
7 that much of a hurdle for them to actually appear in
8 court from anywhere in the world. Again, the enforcement
9 of that is going to be difficult, but -- and as far as
10 the junk fax thing goes, it's more of tracking down who
11 the real Spammer is and it's something that anyone can do
12 if they can find -- through vicarious liability theories
13 where the money's going and then, you know, go against
14 that person. Does that answer your question?

15 MR. GROMAN: Paula wants a word on that.

16 MS. SELIS: Just to follow up on that one, in
17 Washington, small claims courts are courts of limited
18 jurisdiction, and they define themselves by statute. And
19 one of the ways that they define themselves is that they
20 say that you can't bring an out-of-state defendant into
21 small claims court. Yeah, I think it's very common. But
22 you can bring an out-of-state Spam defendant into
23 district court, which is very similar to small claims
24 court. The filing fees are very low, pretty simple
25 procedures.

1 So, I think it's going to vary from state to
2 state, jurisdiction to jurisdiction, whether you can haul
3 somebody into small claims court or not. But it is an
4 issue, and it was an issue in Washington, and as Dietrich
5 pointed out, we clarified in our statute, just this last
6 session, that you could at least bring an out-of-state
7 Spammer into district court.

8 MR. GROMAN: Okay, I'm looking at a lot of
9 glazed faces that appear desperate for caffeine.

10 **(Laughter).**

11 MR. GROMAN: So, I want to thank the panelists.
12 Before we close, I do want to mention that the Chairman
13 made -- mentioned in his opening remarks that the Federal
14 Trade Commission, along with state law enforcement and
15 other federal agencies, are going to be announcing on May
16 15th some new law enforcement actions that will address
17 on-line fraud and Spam. And that will be following up
18 some of the things we've talked about at this forum.

19 So, on that note again, thank you very much to
20 our panelists and we'll see you back.

21 **(A brief recess was taken).**

22 MR. HUSEMAN: Good afternoon. We're finally
23 here for the last panel of three days. And my name is
24 Brian Huseman. I'm a Staff Attorney with the FTC's
25 Division of Marketing Practices. And I just asked who

1 gave me this lousy time slot, but I guess that was me, so
2 I guess I can't complain.

3 **(Laughter).**

4 MR. HUSEMAN: In this panel, we're going to be
5 talking about two very distinct things but two very
6 important topics in our solutions day. We'll be talking
7 about technological solutions to Spam and also structural
8 changes to e-mail. I really see the panel delving into
9 three different phases, and the first will be what
10 current technological approaches can we use to try to
11 solve the Spam problem. And I want this panel not to be
12 a discussion of should someone -- should a consumer or a
13 business buy Spam product A versus Spam product B.
14 That's not a very useful discussion. Instead, we're
15 going to be focused more on the technologies and the
16 approaches themselves, what are the pros and cons of each
17 of these different methods of dealing with Spam in a
18 technical manner.

19 The second phase of the panel will be talking
20 about some specific panels that have been put forth about
21 how we can, with technology, deal with the Spam problem.
22 And then the third phase we'll be talking about some big
23 picture structural changes to e-mail, the way that the e-
24 mail protocol is set up, the way that we communicate with
25 e-mail. And, so, we'll be just tossing some of these

1 ideas out there and evaluating whether they're efficient
2 or even possible to do.

3 This is one area where the FTC, you know, does
4 not have a lot of expertise in, as we're not
5 technologists, we're lawyers instead, but it is probably
6 one of the most important, if not the most important,
7 possible solution to the Spam problem.

8 And I want to point out initially before we
9 start that Ira Rubinstein from Microsoft has been
10 replaced by Ryan Hamlin here on my far right, who is the
11 general manager of the Anti-Spam Technology and Strategy
12 Group at Microsoft, so just make that in your notes.

13 So, we're first going to start out with John
14 Levine. John, will you please show us your presentation?
15 We're going to -- get us all on the same playing field.
16 And I would ask all the panelists, you know, as I said,
17 I'm a lawyer, not a technologist. John is the author of
18 "Internet for Dummies," so that's a good approach and
19 mindset to keep in mind. Let's talk about this from a
20 dummy's perspective at the beginning to examine the
21 various approaches and the pros and cons of each.

22 MR. LEVINE: Thank you, Brian. I'm going -- I
23 have set for myself the simple task of explaining all
24 known approaches to Spam filtering in four minutes, which
25 is not going to happen. But my goal in this little pitch

1 is basically to show you that there's a lot of different
2 approaches that have already been attempted and are
3 already fairly well understood and that people keep
4 reinventing, because there's a very bad habit for people
5 to think that they're the first person ever to invent the
6 idea of a white list or something.

7 So, if we can categorize the approaches, I
8 think it makes it much more -- it will make it much
9 easier to talk about what's promising and what's not
10 promising. And I will attempt to keep my snide remarks
11 about the promisingness of each approach to a minimum.

12 As we move through sort of the stages of
13 processing an e-mail, the first is source filtering,
14 looking at where -- even before you receive the message,
15 looking at where it comes from and how do you decide
16 whether you even want to accept it in the first place.
17 And I have five approaches here. I'm going to explain
18 these very fast, and if you don't understand everything,
19 come and talk to me later, and I'll be happy to tell you
20 in more detail when I can talk slower.

21 The first couple of lists are blacklists.
22 There's a variety of ways that people create blacklists.
23 The first one is mechanical, mechanically generated DNS
24 blacklists. These are things that report -- things that
25 you can test mechanically that are known to be sources of

1 Spam, open relays, proxies, addresses that have sent to
2 Spam-trap addresses.

3 The second category of blocking lists is what I
4 call untrustworthy senders. If a machine is a dial-up
5 user of a consumer ISP, a correctly configured mail
6 system will route the mail through the ISP's mail server.
7 If it attempts to send directly, it means it's either a
8 Linux weenie or it's a Spammer. And Linux weenies are
9 educable, so in general, it makes sense to reject that
10 kind of mail.

11 The third kind of blocklists is what we call
12 shared reports. A lot of people send in reports that
13 they're Spam and based on those reports, it more or less
14 automatically creates a blocklist of the addresses from
15 which the reported Spams came.

16 The next kind of blocking lists are waiting
17 services, Spam sources. These are actually created by
18 human beings who are identifying sources that they
19 believe are sources of Spam or related to Spam, that you
20 probably wouldn't want to receive. And the best known
21 are the SBL and the MAPS RBL, both about which we heard
22 quite a lot yesterday.

23 And the final source filtering scheme is what I
24 refer to as DNS poisoning, which is basically to say if -
25 - when an incoming message has a return address or a lot

1 of domains that appear to send nothing but Spam, and if
2 you simply adjust the mechanics of your internal domain
3 server so those domains can't be found, then your normal
4 reject scheme that rejects mail with impossible senders
5 will reject it.

6 The other kind of poisoning is simply -- if you
7 notice that there are Spammers on a particular network,
8 you can adjust your own domain server so that when they
9 send a request to you to say where do I deliver mail for
10 your domain, it sends back a message saying I don't know,
11 which is -- it's not widely used, but it's quite clever.

12 Once the message is received, now there's a
13 whole bunch of approaches to content filtering, where you
14 actually look at the message to decide whether or not you
15 want to receive it. The first is protocol defects.
16 There's a mechanical definition of the SMTP protocol, and
17 in general, the legitimate software does SMTP correctly
18 and the more defects in the transaction, the more likely
19 it is that it's sloppily written Spamware.

20 MR. HUSEMAN: John, what is SMTP?

21 MR. LEVINE: Oh, it's the optimistically named
22 simple mail transport protocol. It's the scheme used to
23 transport mail from one computer to another over the
24 internet. Sorry.

25 So, first -- again, you can make these fairly

1 mechanical tests, and these are quite reliable. The next
2 is look at the headers of the message, and this is where
3 you come into sender white lists and black lists. If
4 it's from a sender that you know you don't like, you
5 reject it; if it's from a sender that you know you do
6 like, you accept it. And there also turn out to be other
7 kinds of mechanical defects in the headers that you can
8 check for, and again, the more defects you have, the more
9 likely it is that it's Spam.

10 MR. HUSEMAN: John, can we go back to your
11 first protocol defects. What is RDNS?

12 MR. LEVINE: RDNS is the reverse lookup to find
13 out where the message came from.

14 MR. HUSEMAN: So, can you give us an example of
15 how that would work?

16 MR. LEVINE: Yeah, whenever a message comes in,
17 it has, as we saw in the session on the first -- in Nick
18 Nicholas' session in the first day, it has a sender -- it
19 has an address it's routed to and it has a return
20 address. And the return -- what you can do is you can
21 simply look up the return address and say, where would I
22 deliver mail sent back to that return address. And if
23 you don't get a response, you know the return address is
24 forged, and that's a very strong indicator that it's
25 Spam. And, again, my previous thing about DNS poisoning

1 basically makes it look like your own addresses are
2 forged to confuse Spammers.

3 Once you've analyzed the headers, there's
4 various things you can look for in there. Then I think
5 the largest category of Spam filters are body strings.
6 They actually look for pieces of text in the body of the
7 message. These slides are all on my website. I can give
8 you the URL later, so you don't have to carefully copy
9 them all down.

10 There's two kinds of body filters. One are
11 what I call fixed body filters, where the strings are
12 more or less built into the filtering program or they're
13 updated occasionally. The other is what I call adaptive
14 body filtering, which is also known more trendily as
15 Bayesian body filtering, where you simply say here's a
16 whole bunch of Spam, here's a whole bunch of non-Spam,
17 and it uses statistical methods to try and figure out
18 what strings are likely to appear in Spam, what strings
19 are likely not to appear in Spam.

20 Bayesian filtering used to work really well.
21 But since Spammers are not totally stupid, they have
22 figured out to make their Spam look either -- either look
23 more like real mail or to be so short that there aren't
24 enough strings to apply filters to.

25 MR. HUSEMAN: John, so Bayesian filtering,

1 would that be, for example, the same -- if a Spam message
2 has the words free plus money plus offer, then there is
3 an X percent chance that that is actually Spam message?

4 MR. LEVINE: Like that except that it's
5 completely automated by software. You simply say here's
6 all my Spam, here's all my real mail, and it figures out
7 what those likely strings are. And having looked at some
8 of the Bayesian filters that have been generated
9 automatically, they come up with wild stuff, stuff that
10 you wouldn't expect, which frequently turns out for a
11 while at least to be a really good indicator of Spam, at
12 least until the Spam mutates.

13 The next that I find works really well is bulk
14 counting. I use a system called DCC, called short for
15 distributed checks on clearinghouse, where basically what
16 it does is it makes sort of a one-line code number that
17 digests the content of each message. And then a group of
18 DCC servers simply go and count the number of messages
19 with the same signature. And if you have many messages
20 with the same signature and they're not from a known good
21 mailing list, it's probably Spam.

22 Again, I find this extremely effective,
23 particularly I have a lot of e-mail addresses that appear
24 in my books, so they never -- they absolutely cannot
25 legitimately subscribe to any sort of real mailing list,

1 so any bulk mail that comes to those addresses must be
2 Spam. And bulk counting works really well for that.

3 A related thing is what I called shared
4 announcements, where DCC simply counts -- DCC counts all
5 the messages, and you have to make special arrangements
6 for it not to look at your legitimate mailing list.
7 Shared announcements, the best known of which is Vipol's
8 Razor, which has been commercialized as Cloudmark.
9 People send in their Spam, and it attempts to come up
10 with a shared counting system for just counting Spam, not
11 counting all the messages.

12 MR. HUSEMAN: So, John, can you give an example
13 of how that would work practically?

14 MR. LEVINE: Oh, people basically, when they're
15 going through their mailbox, every time they see Spam,
16 they forward it off to the local Razor server. And then
17 it automatically updates the bulk counters that it keeps,
18 so that when future mail comes in, it can say, oh, look,
19 this has the same signature as all these messages that
20 were reported as Spam, therefore it's probably Spam, too.

21 MR. HUSEMAN: So, is this also known as the
22 peer-to-peer or collaborative approaches --

23 MR. LEVINE: It's one of the collaborative
24 approaches. DCC is also collaborative. The difference
25 is that DCC is automatic. It counts everything, and you

1 have to separately figure out what's from a real mailing
2 list.

3 MR. HUSEMAN: Does DCC stand for something?

4 MR. LEVINE: Distributed checks on
5 clearinghouse. It's a tool beloved by weenies.

6 **(Laughter).**

7 MR. LEVINE: It's hard to install and hard to
8 explain, but it works really well.

9 **(Laughter).**

10 MR. LEVINE: Razor particularly in its
11 commercialized form is easier to set up because it's been
12 packaged in a more attractive way.

13 And, finally, what I can only call Spammy
14 behavior, if you have like subject lines with random
15 strings of text and numbers in them and e-mail messages -
16 - you know, I get a lot of e-mail messages that start
17 with sort of long sets of words that clearly mean
18 nothing. Those are called hash busters. Those are
19 specifically put in there to defeat these bulk counting
20 systems, to try to make all the different copies of the
21 Spam look different enough that they're not recognized as
22 the same. However, you can look for hash. There's a lot
23 of hash busters that turn out to be done in really dumb
24 ways, and you can count them and you can identify them.

25 The next approach is hybrid filtering. No

1 single approach works all that well, so we mix them and
2 match them. Some of the best known are Spam Assassin and
3 Mail Shield. I happen to use Spam Assassin because it's
4 free and it runs on the kind of server I use. And there
5 are lots of add-ons to your mail transport agent, the
6 actual mail server software, that you can buy. And I
7 think if you talk to most ISPs, they will -- at least
8 part of their Spam filtering will be home brew, so
9 there's a lot of variation there, too.

10 Now, this next thing starts to approach on ways
11 that we might be changing the way that e-mail works. And
12 sender identification is a way to say that if we know who
13 the sender is and we know it's not somebody we hate, then
14 the mail is most likely good. The best known sender
15 identification are the two cryptographic signature
16 schemes, PGP and S/MIME. They work pretty well, but the
17 fact that they've both been around for years and nobody
18 uses them suggests that they have usability problems.

19 The next possibility is what I call per-
20 correspondent addresses, and there was a blurb out there
21 for one variation, a blurb out in the back, for one
22 variation of this. And basically you give each of your
23 correspondents a different address of yours to send mail
24 to. And then if -- when the mail comes in, if the
25 address it's sent to matches the correspondent you gave

1 it to, you know it's okay. If it comes in to some random
2 other address, or even worse, if you get mail that you
3 gave to person A, but you received mail to that address
4 from person B, that suggests that they sold or
5 transferred your address.

6 So, that can be a very good way to keep track,
7 particularly when you're doing business with companies,
8 all of whom require an e-mail address. It's a good way
9 to keep track of who you're corresponding with. And in
10 my case, I find it's very useful that a message shows up
11 in my inbox and I say ooh, it looks like Spam, and then I
12 say oh, wait, that's the right address, I did business
13 with them a year ago, so I know it's okay.

14 MR. HUSEMAN: So, would this be a disposable e-
15 mail address?

16 MR. LEVINE: You can treat them as disposable.
17 In my case, they're not disposable; either they're active
18 or they go to the Spam trap. But other people treat them
19 as disposable.

20 A related thing to this, actually to the
21 reverse DNS lookup is some mail systems actually when an
22 incoming message comes in from an unfamiliar address, it
23 actually starts a session back to the sending mail system
24 and attempts to deliver -- it goes through the first half
25 of an SMTP session to try and send mail back to that

1 address, to see whether at least the address is accepted.
2 And this is a more sophisticated way to validate that the
3 from address is real. This isn't widely used, and I
4 think this has scaling problems. I think it would be
5 really resource-intensive to use a lot.

6 Another popular scheme that I don't like for
7 reasons that I won't take time to explain is challenge
8 response. When somebody -- you send mail to someone you
9 haven't heard -- you haven't corresponded with before.
10 And his computer automatically sends back a message
11 saying who the heck are you. And if you respond to the
12 challenge in some satisfactory way, and satisfactory is
13 anything from clicking on a link to sending them an essay
14 explaining why you were worthy of their valuable
15 attention. But if you send back a satisfactory response,
16 then you're white listed.

17 There are a variety of trusted sender schemes,
18 and Vince is going to tell us about one, so I won't
19 attempt to describe it. But this is basically a way to
20 say that not only can you identify who a message is from,
21 but some organization who you presumably trust says we
22 have investigated the sender and the sender says that
23 this mail is of such and such a category and from our --
24 as far -- you know -- and we will assert that what he's
25 saying about it is true. So, that can be useful as a way

1 simply to put useful labels on mail, so that mail can
2 identify itself as yes, this is bulk; yes, this is not
3 bulk. And, so, if they lie about it, it's much clearer -
4 - you have a much clearer way to go after them and say
5 not only is it Spam, but you're a liar.

6 And the final one in sender identification are
7 various technical ways that are sort of analogous to the
8 realtime mailback but more technically efficient to
9 verify that the address -- that the internet address that
10 a piece of mail is coming from is a sending server that
11 is authorized to send mail with that return address, and
12 it's simply -- it's a more complicated and more
13 sophisticated way to validate that mail is actually
14 coming from who it purports to be coming from.

15 And, again, it's similar enough to per-
16 correspondent addresses and signatures that we can
17 consider them all together.

18 MR. HUSEMAN: Now, where would the white list
19 approach fall? Would it be a sender identification
20 method?

21 MR. LEVINE: I actually treat that more as
22 content filtering, because partly it's -- well, no, white
23 list is not sender identification because you have no way
24 of knowing that the address that the message purports to
25 be coming from is actually who it's coming from. In

1 other words, you know, if I -- if I know Brian's a good
2 guy and I put his address in my white list, then all mail
3 from you will automatically be white listed. But if some
4 third party then sends me a virus that fakes your address
5 in the return address, it will pass through my white
6 list, even though it's not really from you. So, the
7 point of the sender identification is to distinguish mail
8 that's really from you versus mail that only purports to
9 be from you.

10 MR. HUSEMAN: So, white list would fall under
11 the content filtering. And if you could briefly explain
12 what a white list is.

13 MR. LEVINE: Oh, a white list is simply a list
14 of e-mail addresses from which you believe you want to
15 receive mail. I mean, like everybody in this room, I
16 would guess, would qualify for my white list. You know,
17 so if you send me mail, it will basically say oh, it's
18 from you, I'll bypass all those other filters and I'll
19 just put it in my mailbox.

20 MR. SCHIAVONE: Did you opt in to every mailer
21 in the room?

22 MR. HUSEMAN: Please speak in the mike.

23 MR. LEVINE: Did I -- Vince asked did I opt-in
24 to every mailer in the room. For individual messages
25 telling me how wonderful I am, yes.

1 **(Laughter).**

2 MR. LEVINE: And my final set of possible
3 changes to e-mail are what I call -- are postage schemes,
4 ways to put -- basically, some ways to charge the sender
5 some amount for the privilege of delivering mail to you.
6 And they fall into two large categories. One is what's
7 called hash cash, where there's no money involved but the
8 sender -- you present the sender with a computationally
9 difficult computing problem, which it then has to solve
10 to allow the message to be delivered. And the idea is
11 that solving the message will be time-consuming enough
12 that Spamming people will be too slow, because you'll
13 have to solve too many of these problems.

14 MR. HUSEMAN: Where would that message come
15 from? Would it come from the ISP or from the individual
16 recipient?

17 MR. LEVINE: Ask six geeks, get six different
18 answers. Some people attempt to send the hash challenge
19 back from the mail server; some attempt to send it back
20 from the end-user. I think that it's not practical
21 simply because the computer speeds vary so much, you
22 know, and my stepmother's 486 might take an hour to solve
23 a problem that a Spammer's two-gigahertz Pentium VI could
24 solve in a tenth of a second. So, I think that makes
25 hash cash impractical.

1 The final thing is e-postage, where you put
2 real money on it. And I think -- I think e-postage is
3 impractical just because it requires building a brand new
4 organizational structure like the post office, okay? We
5 already have one of those, and it has its problems.

6 **(Laughter).**

7 MR. LEVINE: You know, so everything -- and I
8 say, like, okay, if you're going to charge people two
9 cents to send you mail, that's fine. Now, when a bad guy
10 puts a virus on your machine that sends Spam to third-
11 parties, who pays the postage? I don't know. Yeah, we
12 can probably solve all these problems, but we're going to
13 take one can of worms and replace it with a bigger,
14 uglier, more expensive can of worms. So, e-postage --
15 everybody says e-postage would be great. I simply don't
16 think that it's implementable.

17 So, anyway, that's my very short overview.
18 And, again, if you want more detail on what these things
19 are the URL where the slides are, come and talk to me
20 later.

21 MR. HUSEMAN: Can you just say the URL briefly?

22 **(Laughter).**

23 MR. LEVINE: www.iecc -- that's I E C C --
24 .com/ftcSpamtech -- T E C H -- .ppt. And if you didn't
25 get that, I'll tell you again later.

1 MR. HUSEMAN: Thanks. Now, Matt Sarrel, you
2 are technical director for PC Magazine's Internet Lab,
3 and so you have examined all of the actual commercial
4 products, both for consumers and business and tested
5 those out. Let's go through John Levine's categorization
6 of all the various technical approaches to Spam and talk
7 about how those approaches have both pros and cons for
8 consumers and businesses and today's actual products that
9 are out there. What about any source filtering products?
10 What are the pros and cons of that approach?

11 MR. SARREL: Source filtering works fairly well
12 on a system level. The only -- the immediately
13 noticeable problem to source filtering is when sending
14 systems get placed on blacklists incorrectly, which
15 actually, interestingly enough, happened to Ziff Davis --

16 MR. HUSEMAN: Which we talked about yesterday,
17 had a sense of discussion kind of about that problem in
18 one of yesterday's panels.

19 MR. SARREL: So, they can be helpful, but
20 they're not the answer to the whole problem. And they're
21 also, from a computational sense, they're relatively easy
22 to implement and not very costly.

23 MR. HUSEMAN: What about content filtering?
24 So, this would include various things such as white
25 lists. Let's talk about white lists first. What are the

1 pros and cons of that approach?

2 MR. SARREL: I think one of the major pros to
3 white listing is that it's a very easy concept to
4 understand. So, it's sort of like you say this is a list
5 of people that -- for whom I'm willing to accept e-mail,
6 and whatever they send me, I'll accept. Now the problem
7 is, when someone ends up on your white list who doesn't
8 belong there, and the other problem is what happens when
9 you add someone to a white list based on an ambiguous e-
10 mail.

11 One of the problems that we had in our testing
12 is that the actual definition of Spam, so what's really
13 Spam, what do you really want, what do you really not
14 want. And we happened to get an awful lot of e-mail that
15 we called gray Spam, which is Spam that we didn't ask
16 for, but we read and it turns out to be relatively
17 interesting.

18 **(Laughter).**

19 MR. SARREL: That doesn't happen to everyone,
20 but being in the media, I get e-mail every day from
21 someone I've never met who wants me to look at their
22 product. And if I start rejecting everything that comes
23 from someone I don't know, then that's going to affect my
24 business.

25 MR. HUSEMAN: Do you think that white lists are

1 practical for businesses, as opposed to consumers?

2 MR. SARREL: No, I do not. I think white lists
3 may play a role in the consumer market, primarily because
4 it's very easy to understand. You just put all of the
5 people that you trust already into your white list, and
6 you receive mail and you can look at that. But then you
7 run into the situation of what happens if a long lost
8 friend finds you in some kind of e-mail directory and e-
9 mails you and they're not in your white list. So, then
10 even though you have the white list, you still have to
11 dig through all your quarantined e-mail. The white list
12 is a start. I think actually white lists and blacklists
13 are a start, but they're not an answer.

14 MR. HUSEMAN: Dan Tynan, you are contributing
15 editor of PC World, and you've also examined the various
16 approaches, technical approaches to Spam, as well as
17 you've also looked at the world of Spamming and some
18 particular Spammers as you described them as well. Let's
19 talk about some more content filtering, and specifically
20 content filtering based upon certain words, their
21 messages. What are the benefits and also the negatives
22 to that type of approach?

23 MR. TYNAN: Well, I would say that that's kind
24 of been the traditional form of Spam filter for a long
25 time has been content filtering, where it looks for words

1 like Viagra and worse. We all know what they are. I'd
2 say the sort of the flavor du jour is really white list
3 and challenged response. The last three or four products
4 I've looked at have been exactly that. And that seems to
5 be where the thing is going. I think that's also a
6 response to the fact that content filtering is
7 continually defeated by Spammers.

8 One example is, you know, a product like Spam
9 Killer. Spam Killer will look for words and phrases. It
10 has something along the lines of 5,000 different content
11 filters. And, so, it will look for the word Viagra, and
12 so Spammers will then put the word Viagra with a little
13 star between each letter, so they have to change the
14 filter. And then they'll put it inside HTML code, and so
15 they'll have to change the filter. And then they'll put
16 an HTML tag in the middle of the word Viagra that's
17 invisible but defeats the filter, and so they have to
18 change the filter. So, it's a constant game of cat and
19 mouse. As a result, my testing, content filters out of
20 the box, 80 to 90 percent effective.

21 MR. HUSEMAN: And I address this issue, let's
22 say, to John Levine. Is 80 to 90 percent effective
23 filter good enough?

24 MR. LEVINE: It kind of depends on who you are.
25 If you get ten Spams a week, you know, and it knocked you

1 down to one, then that's -- you're in pretty good shape.
2 I've had the same e-mail address for ten years, so I get
3 a lot of Spam. And in my case, you know, if my Spam
4 filter is running less than like 98 or 99 percent
5 accurate, I'd have some -- my regular inbox would still
6 have more Spam than regular mail.

7 MR. HUSEMAN: What about the issue of Spammers
8 using -- or sending a message that has only an HTML
9 image, so there are basically no text words in which to
10 filter? Can these filters solve that problem?

11 MR. TYNAN: There are some filters that do that
12 look for specific HTML characteristics. Spamnix is one
13 that does that. I think Spam Assassin also does. And,
14 so, they have a waiting system, they assign points and
15 say, okay, if it has this kind of image, then it assigns
16 X number of points. And when it reaches a certain point
17 threshold, it says, okay, this is probably Spam, and it
18 shuttles it off into a Spam folder.

19 MR. HUSEMAN: What's your response to that,
20 Matt? Do you agree?

21 MR. SARREL: Oh, with that particular kind of
22 Spam, which is just an HTML image, that's really easy to
23 filter, since no one ever sends you real mail that looks
24 like that. The issue is how hard is it to update your
25 filter to recognize the Spammer gimmick of the week, and

1 it's more of a software maintenance problem than a
2 technical ability to deal with that particular kind of
3 Spam.

4 Right now, that's the constant battle, is
5 what's the Spam flavor of the week. Is it V/I/, or is
6 V*I/, or is it Spam sent to me from another country in
7 another language, or is it a graphic. That's -- right
8 now, that's where the war seems to be fought, is can the
9 Spam filtering products keep up with the Spammers.

10 MR. HUSEMAN: I guess one question I want to
11 pose is that if this is an 80 to 90 percent effective
12 solution, what are the -- first of all, is this solution
13 good enough because of the continual updating and trying
14 to figure out what the new Spammer tactic is.

15 MR. SARREL: Well, one thing that we did when
16 we looked at these products, we looked at the consumer
17 products and we found them to be roughly between 75 and
18 85 percent effective. And then we looked at the ISP or
19 corporate products, and they were roughly between 85 and
20 95 percent effective. And we said well, that's
21 significantly better.

22 But then if you think about it, if you're --
23 like John was saying, if you're a consumer and you get 10
24 Spam messages a day and this software filters them out
25 and now you're only getting two, that's great. But what

1 if you're an actual company and at this point you're
2 getting 10,000 Spam messages, you know, in a week. So,
3 now what are you filtering out? You still end up with a
4 thousand Spam messages. So, I think it's not necessarily
5 as important to filter out -- the statistics are more
6 interesting than just who's catching the most Spam. It's
7 whether the legitimate mail is making it into your inbox,
8 so in other words, avoiding a false positive, which in a
9 business sense could be very costly. And it's also --
10 like correctly diagnosing a true Spam..

11 MR. HUSEMAN: Let's now talk about the
12 technical approach, the collaborate or a peer-to-peer
13 approach. This is where consumers or individuals vote on
14 what they think is Spam and then based upon the aggregate
15 statistics that message is labeled as Spam and then
16 filtered or blocked out. Dan Tynan from PC World, what
17 are the pros and cons to that?

18 MR. TYNAN: Well, the one that I've used
19 personally is Cloudmark Spamnet and when I started it, it
20 caught about 66 percent of the Spam. And it's one of
21 those products that you have to continually use and tweak
22 and you submit -- you know, you get a piece of Spam, you
23 click on it, you submit it back to Cloudmark, and
24 eventually they develop what they call a trust rating,
25 whether you are a trustworthy sender of actual Spam. And

1 as your trust rating grows, they give more weight to your
2 submissions. So, eventually they decide that you know
3 what you're talking about and that they will start
4 blocking the Spam for you and for everyone else that you
5 submit. But it takes a while. You know, I didn't test
6 it long enough to really see the improvement. People who
7 were here this morning heard John Patrick on a panel
8 earlier who claimed he had 99.9 percent Spam protection.
9 He uses Cloudmark Spamnet.

10 MR. HUSEMAN: Ryan Hamlin at Microsoft.

11 MR. HAMLIN: One comment, we use at Microsoft
12 collaborative filtering, and that's the version that will
13 be shipping now with Outlook and with our next version of
14 MSN. What we like about collaborative filtering is that
15 it's not dependant on a specific set of words, like
16 Viagra, right? There's a bucket of good mail and a
17 bucket of bad mail. And in that bucket of bad mail,
18 maybe the combination M, dash, period, space, space, Y
19 has shown up in many bad mails, and so it's based on
20 that. And, so, it's not as prone as rules-based human
21 error, because it's based on a large sampling of what
22 users identify as good mail versus bad mail.

23 The key point, too, is that it has to have a
24 mechanism of realtime, because as you know, it's a
25 countermeasure, a battle that we have with the Spammers.

1 And, so, the nice thing about collaborative filtering, it
2 is near realtime, and so you're constantly training your
3 filters on a frequent basis to react to that Spammer, and
4 so when they find a way around it, you know, little be
5 known to the Spammer, you know, the next day we have a
6 new train filter that has caught. And, so, there's a lot
7 of advantage, we believe, in the collaborative filtering
8 approach.

9 MR. HUSEMAN: I would just make one point. You
10 know, again, we're not here to talk about the pros and
11 cons of various products, but instead various approaches.
12 And with that, John Levine, I have one question, and then
13 I'll let you have a response as well. Is this too hard
14 for the average user, this type of approach?

15 MR. LEVINE: Given how successful AOL has been
16 with their report Spam button, probably not. And people
17 are very happy to say -- people are very happy to have a
18 hammer they can use to hit their Spam with. However, I'm
19 worried that Spammers are adapting and collaborative
20 filtering is becoming less effective.

21 The granddaddy of collaborative filters is a
22 system called Brightmail, where they have Spam-trap
23 mailboxes, mailboxes that are legitimately used for
24 anything but seeded on the web pages and stuff. And from
25 these Spam-trap mailboxes, they get vast amounts of Spam,

1 all filtering back to Brightmail's headquarters, where
2 they have three shifts of highly trained geeks looking at
3 the stuff coming in and updating filters in realtime that
4 then are shipped out to filtering servers that their
5 customers use.

6 And it's a great concept, and when Brightmail
7 first came out, it was a killer. It caught all the Spam.
8 But looking now, I happen to have a few mailboxes that
9 are behind Brightmail filtering, and now it catches maybe
10 two-thirds of the Spam, you know, and Brightmail -- and
11 Brightmail is run by very competent people. And, so, I
12 am -- I have some doubt that collaborative filters in the
13 long run can do much better than that.

14 MR. SARREL: There is one advantage to
15 collaborative filtering, though, which is that if it's
16 not catching all the Spam, it's certainly not creating
17 any false positives.

18 MR. LEVINE: It's negligible, yeah. The only
19 time you get a false positive is when you report a Spam
20 and then the ISP writes back to you with a response. It
21 happens to quote the Spam that you reported. But that's
22 actually easy to white list.

23 MR. HUSEMAN: I just have one point of
24 clarification. A false positive, of course, is a message
25 that is labeled as Spam that is, in fact, not Spam. On

1 these collaborative approaches, though, if it's up to the
2 individual to label something as Spam, you know, as we've
3 been talking about for the past three days, no one can
4 really agree on a definition of Spam, so how can there be
5 no false positives if it's up to the individual to report
6 each message as Spam.

7 MR. LEVINE: Generally, the number of people
8 that you are accepting reports from is large enough that
9 the only ones that pass the filtering threshold is stuff
10 that everybody agrees is Spam.

11 MR. HUSEMAN: Now let's talk about some of
12 these sender identification approaches. And, Dan Tynan,
13 what about the challenge response system? Does this work
14 and what are the pros and cons of that?

15 MR. TYNAN: Well, I tested a challenge response
16 system recently, and I heard back from a couple of people
17 who said why are you challenging my e-mail? Why are you
18 inhibiting my ability to communicate with you? And I
19 said it wasn't me, it was my filter. But they had a
20 valid point, and, you know, that is one major problem
21 with challenged response. Another problem is dealing
22 with automated e-mail. I get a lot of it. I'm on a lot
23 of newsletter lists, and challenged response really
24 doesn't work there. You have to manually add them to
25 your white list. And, you know, it's not infallible.

1 Until recently, I would have said, you know,
2 the advantage for white list with challenged response is
3 it's 100 percent effective, but I tested one recently and
4 I got some Spam, and they were on my accepted sender
5 list. And I have no idea how they got there. But I'm
6 trying to find out.

7 MR. HUSEMAN: Matt Sarrel, will senders of
8 messages that receive a challenge, will they respond to
9 those messages, or is that too much work?

10 MR. SARREL: I think it's too much work. In my
11 experience, having run several of their products that
12 rely on challenged response, there are a few things to
13 consider. One, if the person -- if the sender doesn't
14 quite understand the challenge response method, then they
15 don't really know what's going on. They don't know if
16 it's a legitimate challenge. And, also, it may not even
17 make sense to them, at which point they'll just hit
18 delete. They won't understand that you didn't actually
19 get their original message. And the other thing with a
20 challenged response is that they're not perfect. One of
21 the challenge response products sends you an e-mail, how
22 many kittens are in this picture, and guess what, no
23 matter what you answer, it accepts that as a valid
24 response.

25 **(Laughter).**

1 MR. SARREL: So, there's actually a pretty easy
2 way around that. And, finally, one other thing that
3 concerns me a great deal is that the other day, while I
4 was testing this challenge response, I got an e-mail, I
5 sent a challenge back, I got a response back that
6 included a challenge.

7 **(Laughter).**

8 MR. SARREL: And that wasn't a good system.

9 **(Laughter).**

10 MR. HUSEMAN: John Levine, what is your
11 thoughts on the challenge response?

12 MR. LEVINE: I don't like them at all. Partly
13 it's that, you know, they're insulting. Somebody's
14 saying I'm much too important to listen to you unless you
15 beg. Partly it's that they tend -- is that they're very
16 difficult to implement without making egregious mistakes.
17 Every time I write to a large mailing list these days, I
18 always get back a couple of challenges from broken
19 challenge systems that don't recognize that it's mail
20 from a mailing list.

21 I think challenge -- something like challenge
22 response could work, but it would have to be more -- but
23 it would have to be one where the challenge was not sent
24 as e-mail but it was sent by some other scheme that
25 couldn't be misinterpreted as e-mail. And this gets back

1 more to things more like trusted sender, where you --
2 where basically the challenge goes back to sort of a
3 separate place that says was this message really from
4 you, but not sent as e-mail. Those -- you know, those
5 could be built on principle, but not many of them really
6 exist yet and they're not widely enough deployed to be
7 widely useful.

8 MR. HUSEMAN: Talking about trusted sender, Dan
9 Tynan, what are the benefits to consumers and some of the
10 negatives of using a trusted sender program?

11 MR. TYNAN: Well, trusted sender generally
12 relies on a large number of people using the same system.
13 I think the main drawback would be critical mass in that
14 case.

15 MR. HUSEMAN: Can you explain that a little bit
16 more?

17 MR. TYNAN: Well, the system -- for example,
18 there's a system done by Habeas, and I'm willing to bet
19 that Ann Mitchell is here, that inserts copyrightable,
20 trademarkable material into the header of an e-mail
21 message. It actually inserts a poem, a haiku. And
22 people who sign a license agreement to use this can
23 insert the text into the headers of their e-mail
24 messages, and then that's identified as a verified
25 certifiable sender. And people who fake it, people who

1 are Spammers who put the haiku in, can then be sued for a
2 lot more money than they could be sued under normal law,
3 because they're breaking, you know, copyright law.

4 And, so, this is a disincentive. And this has
5 already happened. You know, Habeas has already sued
6 people. So, the advantage there is you do have a -- you
7 know, not only a way of identifying good actors, but you
8 also have a means of redressing bad actors. The bad part
9 is you really need everybody using the same system.

10 MR. HUSEMAN: So, if you were a consumer who
11 used a trusted sender program, and there is currently --
12 let's say that there's not a current system that has a
13 critical mass of users that you can trust, how is that
14 practical? Can you only -- can you accept mail from
15 trusted senders and no one else? I mean, what are the
16 issues here?

17 MR. TYNAN: You know, I'm not familiar enough
18 to really give you the details on it. I think one of the
19 presentations later involves trusted sender.

20 MR. HUSEMAN: Matt, what's your thoughts on the
21 trusted sender technological approach?

22 MR. SARREL: I'm in agreement with Daniel that
23 it's going to be a critical mass issue. And, also, one
24 thing that I see is how much do you trust the trusted
25 sender? So, is that -- like, is that going to be the

1 next Spamming technique, how to get around a trusted
2 system, and perhaps Vincent will shed some light on that
3 later.

4 MR. SCHIAVONE: I'd be happy to.

5 **(Laughter).**

6 MR. HUSEMAN: Now let's take a moment for
7 questions about these various approaches, before we move
8 into our structural changes to e-mail portion of the
9 panel. And, again, as I reminded the panelists, I'd ask
10 the audience members who are asking questions, let's not
11 have your questions be commercials, but let's have them
12 as actual questions and discussions about these
13 approaches.

14 Does anyone have any questions about some of
15 these various approaches currently? Yes, way in the back
16 over here.

17 MR. FERMANSKY: McLean Fermansky, I-space
18 Research Labs. Gentlemen, I'm afraid that your
19 technological solutions don't solve one problem that
20 still stands. It's been alluded to a few times,
21 mentioned a couple of times, and that is cost-shifting.
22 I'd like to use the figures from Mr. Lewis from Nortel.
23 If he were my ISP, he would be running a machine and
24 hiring personnel to carry 400 percent more traffic than
25 he would have to otherwise, if there weren't Spam.

1 Now, Chris is a nice guy, but he's a
2 businessman, as my ISP, and he's going to be charging me
3 for that. Likewise, his upstream provider has to carry
4 that bandwidth, charges him, he charges me. Gentlemen,
5 your solutions only handle Spam that has arrived. I may
6 have a 100 percent effective filter, but it only works on
7 the Spam that's arrived and it doesn't do anything to
8 stop that traffic, to block that bandwidth.

9 MR. HUSEMAN: John Levine, what's your response
10 to that?

11 MR. LEVINE: To a large extent, you're right.
12 In the source filtering approaches tend to knock away --
13 knock down much of the cost by preventing you from
14 receiving the mail, but, I mean, all these filtering
15 techniques fit into the current -- the current design of
16 mail, which as we -- as somebody commented yesterday, the
17 fundamental model is one of the sender freeloading on the
18 recipient. And to fix the cost-shifting requires some
19 fairly fundamental -- deeper changes to the structure of
20 e-mail than we had discussed so far.

21 And I think we can look at them, but I think
22 it's not -- I don't think it's a very promising approach,
23 just because I think that that deep a change to the
24 structure of e-mail, both is something that we don't know
25 how to do and something that even if we did, it took us

1 10 years for people to move from random proprietary mail
2 systems to SMTP, and I'm afraid it would take 10 years to
3 move from SMTP to anything else.

4 MR. HUSEMAN: Vince Schiavone from ePrivacy
5 Group.

6 MR. SCHIAVONE: Well, a couple of things.
7 There is technology available that goes in front of the
8 receiving servers that can analyze traffic paths and, in
9 fact, reverse the economics by slowing the ability to
10 deliver. Right now the economics of Spam are delivery
11 over time. And much of the Spam-fighting -- the Spamming
12 technology moves on if the connection and receipt is too
13 slow on the uptake. So, by analyzing it, you could call
14 it a pre-filter or a squelching technology. You can then
15 slow up the Spam and inhibit their ability to deliver as
16 much and their profit and reduce the costs on the
17 enterprise or the ISP.

18 MR. HUSEMAN: Paul Judge?

19 DR. JUDGE: The question was about cost-
20 shifting, and I think the person asking the question was
21 alluding to some of the technologies that add a monetary
22 cost to sending e-mail, but I believe there's other ways
23 to shift the cost and really aim at the profit of the
24 Spammers without necessarily introducing a cost for e-
25 mails. I think that a number of solutions that we're

1 working on, even detection systems, focus on shifting the
2 cost, at least reducing the profit of Spammers.

3 If you look at Spamming, it comes down to a
4 business, and it's about making a profit and what that
5 entails is the amount of money that the Spammers make,
6 minus the amount of money that it costs them to send the
7 Spam, and the amount of money that they make is affected
8 by a couple of parameters. And one of those is the
9 number of Spam messages that are actually received by
10 end-users and the response rate.

11 So, the number of messages that are received,
12 we have the ability to affect that by the effectiveness
13 of our Spam filters and also the deployment percentage of
14 Spam filters. The response rate, we have the ability to
15 affect that with best practices and user education. And
16 then some of the other costs that we're able to introduce
17 into the system are kind of the cost of litigation and
18 the legislation and going after the Spammers in that
19 manner.

20 MR. HUSEMAN: With this panel, we're really
21 focusing on kind of the technological issues in regard to
22 cost-shifting. Is there a technological way to -- what
23 would you recommend?

24 DR. JUDGE: So, what I just mentioned was that
25 there's two variables that we can affect with technology,

1 and it's really the number of messages received, and that
2 affects the profit that they make. The number of
3 messages sent affects the amount of money that it costs
4 to send out that Spam flood, and the number sent minus
5 the number received is affected by really the
6 effectiveness of your Spam filters and the deployment or
7 percentage of the Spam filters. So, just saying that
8 even without introducing a system that charges for e-
9 mail, we have the ability to affect the profits of
10 Spammers.

11 MR. HUSEMAN: Steve Atkins from Word to the
12 Wise and SamSpade, what is your thoughts on technological
13 solutions to cost-shifting?

14 MR. ATKINS: Not so much to cost-shifting
15 specifically, but in regards to rolling out new
16 protocols, yeah, it took many, many years to go from
17 proprietary e-mail to SMTP, but compare that with instant
18 messaging. If the consumer, the user of the new
19 protocol, sees the advantages of it as being huge, then
20 you can roll out new protocols very quickly.

21 Currently, SMTP is being used for an awful lot
22 of things, perfectly legitimate things and some Spam as
23 well, but it's just really not very well suited to. If
24 some of the traffic that currently is going over SMTP
25 were rolled off onto a more appropriate protocol and it

1 was backed by AOL, Microsoft, Earthlink, Yahoo, Hotmail,
2 then I could see new protocols being rolled out in months
3 rather than years.

4 MR. HUSEMAN: We're going to get to that in
5 just a little bit about some of the protocol changes.
6 Matt Sarrel, what about the current technological
7 approaches that we have and reversing the cost-shifting
8 in Spam?

9 MR. SARREL: We had looked at a number of
10 gateway devices, which Vincent mentioned, and these
11 function similar to -- if you think about a firewall, at
12 the edge of your network, in front of your mail server or
13 in front of the ISP's mail server, and so what they do is
14 not only do they filter the content of e-mails and they
15 can also utilize white lists and blacklists, but there
16 can also be the reverse DNS queries to make sure that the
17 sender is legitimate. And they also look at SMTP traffic
18 that is abnormal, such as someone trying to harvest e-
19 mail addresses from your system using random characters.
20 That's not a typical behavior when trying to send a
21 message.

22 So, if you deploy a gateway device, then that
23 keeps the e-mail from getting onto your systems and using
24 up your resources, which does not entirely address the
25 issue of cost-shifting. However, I think part of the

1 problem is that when we all go out and develop our anti-
2 Spam products, we want to give people something that they
3 see. So, if you -- you know, there's a big differences
4 between a product that you install on your desktop and
5 the next day you see it stopped two-thirds of your Spam
6 and a product that gets deployed at an ISP and it takes a
7 year or two and then we stop getting Spam. I think that
8 the whole product development cycle is part of the
9 issues.

10 MR. HUSEMAN: I have one quick question for
11 some of the panelists, and then we're going to move on to
12 some of the specific technological approaches that are
13 being proposed currently. Let me ask John Levine, let's
14 say your grandmother, to use a grandma example again, is
15 setting up an e-mail account. What approach would you
16 advise her to use?

17 MR. LEVINE: I'm thinking about my dear
18 stepmother, who's a very smart lady, but her expertise
19 is not in computing. And at this point, I would tell her
20 to use an ISP who's got built-in Spam filtering that she
21 doesn't have to mess with, because as someone else
22 commented, the person running the mail server can do a
23 lot better job of filtering than the end-user, just
24 because it has a lot more data at its -- to use, and it's
25 got a lot more compute power to throw at it. And at this

1 point, you know, there's not much more useful that I can
2 tell her.

3 MR. HUSEMAN: Now, Dan Tynan, let's make the
4 example now your teenage son or daughter.

5 MR. TYNAN: Okay.

6 MR. HUSEMAN: What approach would you tell them
7 to use?

8 MR. TYNAN: I think I'd just lock them in their
9 room away from the computer.

10 **(Laughter).**

11 MR. TYNAN: I'm hoping to do that anyway.
12 They'd be more sophisticated, they'd be much more savvy.
13 So, there won't be the technological barriers there are
14 for John Levine's dear stepmother. But they will still
15 be faced with a problem that the off-the-shelf Spam
16 filters and the built-in Spam filters in things like AOL
17 and Yahoo and MSN just don't -- aren't 100 percent
18 effective.

19 So, my point of view on this is the whole
20 purpose of Spam filtering software is to kind of turn
21 back the clock five or six years, to the point where when
22 we used to get e-mail and not Spam, at least not very
23 much of it. And, so, it should be as close to mimicking
24 that as possible, which means I would recommend something
25 that goes right into the e-mail program you like to use,

1 filters it automatically and requires minimal
2 interaction.

3 Unfortunately, most Spam filters require some
4 interaction, because you have to look for false
5 positives, but that's the approach I would go to. I
6 would say okay, look at your e-mail program, your client,
7 whether it's Outlook or Outlook Express or Eudora, find
8 one that filters Spam inside that program with one or two
9 clicks and go for that one.

10 MR. HUSEMAN: Matt Sarrel, let me ask you this
11 question. What approach would you recommend for yourself
12 or approach do you think works the best, or approaches?

13 MR. SARREL: Well, I'll tell you what I do.
14 It's sort of along the lines of the disposable e-mail
15 address model. And this, by the way, is just what I do
16 personally. For work, we have this situation where I
17 need -- I basically need to receive Spam, because some of
18 it is a product announcement. Whether there's value in
19 that or not, I won't comment.

20 So, what I -- I have three e-mail addresses.
21 One is sacred. I don't give that out to anyone except
22 for my friends. And you could sort of think of that as
23 the white list model. And I don't -- I actually have not
24 yet gotten any Spam there. The next account I have I use
25 when you have to sign up for something, like -- but it's

1 something that you might want, like a newsletter or a
2 shipment confirmation, an order confirmation, something
3 like that. I get more and more Spam in there. And the
4 third one is an address that I have where this is, you
5 know, go ahead, Spam it, I check this once every two
6 months just to keep it active, and it's where they force
7 me to sign up for something, just to check a website, or
8 if, you know, someone's giving something away and they
9 need an address.

10 So, it's three levels of sort of what you would
11 think of along the lines of like trusted sender or white
12 lists. And admittedly, that's complicated. Like I
13 wouldn't expect my mother or John's stepmother to be able
14 to handle the three-address system.

15 MR. HUSEMAN: Let's change topics a little bit.
16 Ryan Hamlin from Microsoft, you're the manager of the
17 Anti-Spam Technology and Strategy Group there. As we
18 know, AOL, Microsoft and Yahoo just came out with several
19 proposals, and the proposal had four parts. I want to
20 ask you about some of the specifics about that. The
21 first one -- your first approach was protecting consumers
22 from receiving Spam, and you talked about using the
23 domain name system to better identify the location from
24 which e-mail is originating. What does that mean and
25 what is your proposal?

1 MR. HAMLIN: I'll speak as best as I can on
2 behalf of the other companies, but defiantly should
3 follow up with AOL and Yahoo, because I don't want to
4 misrepresent them. So, from a Microsoft standpoint and
5 what we kind of got out of this alliance is that around
6 the best practices for protecting our consumers, we
7 thought DNS made a lot of sense, because it's global.

8 MR. HUSEMAN: And DNS is?

9 MR. HAMLIN: DNS, domain name servers --
10 server. So, it's global, it's distributed, it's well
11 understood today and it really is the means obviously for
12 the identification today.

13 MR. HUSEMAN: And, so, the DNS is where the
14 internet protocol address matches up with the domain
15 name?

16 MR. HAMLIN: Give it a domain name and get the
17 -- exactly, get the IP address back. So, we felt like we
18 want to leverage an existing technology that's well known
19 and well understood and distributed. And there's
20 multiple approaches to that. We talked about RDNS. I
21 know John talked about reverse DNS as one way of
22 potentially doing that. I mean, with this identity
23 crisis, domain spoofing is one of the biggest issues that
24 we need to really focus on in the short term. We believe
25 that solving a lot of the identity issues will help -- is

1 a big step forward on reducing Spam.

2 MR. HUSEMAN: So, how does this proposal do
3 that?

4 MR. HAMLIN: So, what we've said is that we
5 want to leverage DNS and that we need to get in the room
6 with others, because certainly Microsoft, AOL and Yahoo
7 don't want to dictate to the industry exactly what to do.
8 We want to definitely open this up to other independent
9 parties and the consumer groups and the marketing
10 organizations to get some feedback to us, but the idea is
11 either via reverse DNS, to make sure everyone has a
12 reverse DNS entry, so to John's point, when you do a
13 reverse DNS, there actually is an entry there and you can
14 associate the IP to the domain. Another approach that --
15 and this is a Microsoft approach that we've just kind of
16 thrown on the table -- is to put the IP addresses in the
17 text field in DNS, again, the idea being --

18 MR. HUSEMAN: What does that mean?

19 MR. HAMLIN: So, much like the example I think
20 on the first day, where they spoofed -- I think it was
21 the gal from Yahoo that spoofed basically a mail coming
22 in to the FTC, and basically pretended to be somebody
23 from FTC and the mail coming in, and even though she was
24 logged -- actually, it was an AOL person -- even though
25 she was logged into the AOL domain and had an AOL IP, she

1 was spoofing that she was coming actually from ftc.org.

2 So, by having this solution, what the ISP would
3 do or the in-bound receiver of that mail would do, would
4 do a lookup and say this person claims to be from
5 Hotmail, this person claims to be from ftc.gov, what is
6 the associated outbound IP addresses that they send mail
7 from, does it match? Oh, it doesn't, so in that case, it
8 wouldn't have matched, because that IP would have come
9 back as an AOL IP, and it would have been matched to the
10 wrong domain, an ftc.gov domain. And, so, instantly you
11 would have known that that was Spam and you could junk
12 that mail.

13 MR. HUSEMAN: So, if one was sending e-mail
14 from an AOL domain name, yet it was actually coming from
15 a Hotmail IP address, then you would be able to tell
16 that?

17 MR. HAMLIN: Correct.

18 MR. HUSEMAN: And prevent that form of
19 spoofing? But this proposal would not prevent someone --
20 that has an actual Hotmail account in using a Hotmail IP
21 address from spoofing one of the other millions of
22 Hotmail users? I mean, is that right?

23 MR. HAMLIN: Agree. I mean, this is going to
24 be, you know, a multi-step approach. We believe that
25 this is a great first step forward. We also believe that

1 a lot of the terms of use and the policies that are in
2 place at the ISPs, by having this step forward, it will
3 give the ability to really screen that out. And if
4 within each of the ISPs, I can just speak for Hotmail
5 today, one of the things we've done is we've locked down,
6 for example, you can only send 100 mails a day. So there
7 are certain things within the ISP, then, you can take the
8 next step once you've got the identity crisis kind of in
9 order.

10 MR. HUSEMAN: Steve Atkins, what -- is this
11 effective? Will this do anything for the average
12 consumer's inbox?

13 MR. ATKINS: Well, it will break e-mail. This
14 is basically a variant on designated sender, which has
15 been discussed fairly widely recently on a number of
16 mailing lists where people are discussing this sort of
17 approach. And while it looks tempting on the surface,
18 there are some fundamental bits of e-mail that can break,
19 like e-mail forwarding, e-mail exploders, mailing lists,
20 if it's not implemented absolutely perfectly.

21 MR. HUSEMAN: And what do you mean by those
22 things, e-mail forwarding?

23 MR. ATKINS: Well, if you sign up for -- if you
24 have an e-mail account and you don't want to actually
25 receive your e-mail there, you want to forward it on to

1 your new ISP, you can tell your old ISP to forward the
2 mail on, depending on how that is implemented, it can
3 look to the receiving new ISP like the incoming mail is
4 Spam. At that point, if the new ISP is using a
5 designated sender type protocol, it could mistakenly
6 discard all the mail that was forwarded from your old ISP
7 as Spam.

8 MR. HUSEMAN: Ryan Hamlin, what's your response
9 to that?

10 MR. HAMLIN: So, agree that the way that you
11 set it up, we need to have explicit directions. There's
12 actually, you know, plenty of ways around that, both RDNS
13 and the idea of embedding IPs in a text field. One
14 solution would be embed additional IPs. You don't just
15 put, you know, your mail server IP. If you use an ISP to
16 send your mail for routing, you would have their IP's
17 address in there, as well. So, you would basically allow
18 for in that text field multiple IPs to get around the
19 scenario that Steve described. It's a very real
20 scenario. You would just need to be careful and have
21 explicit instructions and well known in the industry of
22 how to implement that.

23 MR. HUSEMAN: Steve Atkins, do you think that
24 consumers will do this or will be able to do this?

25 MR. ATKINS: This isn't something consumers

1 would do. This is something ISPs would either choose to
2 do or not choose to do. It's an interesting concept and
3 a lot of people are interested in playing with it. How
4 much of the network it will break when it's deployed,
5 we're probably not going to find out until somebody
6 deploys it and sees.

7 MR. HUSEMAN: John Levine, what are your
8 thoughts on this proposal?

9 MR. LEVINE: I'm actually with Steve here,
10 because I've -- this is -- in my taxonomy, this is what I
11 referred to as designated sender, list the valid places,
12 list the approved places that mail from certain domains
13 can come from. It's certainly a way to keep down on
14 spoofing. But, I mean, certainly on my own network I
15 have a lot of indirect web hosting customers, and mail
16 sent to webmaster@, you know, whoever it is, is then
17 remailed off to wherever their actual ISP account is, and
18 all of that mail will be broken by a straightforwardly
19 implemented designated sender scheme.

20 I mean, I think there are ways around it, but
21 for a lot of these changes, you really have to weigh off
22 -- you have to balance to what extent will this break the
23 way that mail works today and is the cost of that
24 breakage worth whatever benefit it's going to provide.
25 And in the case of designated sender, I think the jury is

1 still definitely out. I couldn't tell you either way.

2 MR. HUSEMAN: Ryan Hamlin, what does Microsoft
3 see as the implementation and the timing of this change?

4 MR. HAMLIN: That kind of approach? So, like I
5 said, I mean, we want to make sure that -- there's a lot
6 of really smart people, and we've had a lot of great
7 opinions and debate about this. I think it's very
8 important, events like this are great because it will
9 force us to move in a quick manner. And I agree with
10 Steve, we need to do some of this trial and error to get
11 it done. So, our plan is, again, to quickly open this up
12 to others. Again, we don't want to just dictate it,
13 Microsoft, or Yahoo or AOL, and get some additional
14 feedback and opinion from others, but then we look for a
15 short time frame to try it out, because we think that's
16 an important next step.

17 MR. HUSEMAN: Paul Judge from the Anti-Spam
18 Research Working Group, which we will talk about in a
19 moment, but what are your thoughts on this particular
20 proposal?

21 DR. JUDGE: So, within the Anti-Spam Research
22 Group, a number of things we're looking at. One of them,
23 of course, is authentication, and we do have a very
24 similar proposal that has been put on the table and
25 designated sender, we refer to it as reverse MX lookup.

1 There's reverse DNS. I think what he just described
2 refers to a reverse MX lookup. And I think that it's
3 something that can be deployed incrementally.

4 It doesn't require that one day everyone turns
5 it on and we begin to drop the rest of the e-mail and
6 break e-mail. If a domain decides to turn it on, then
7 they've prevented forgery for their domain and they're
8 protected. For persons that have not turned it on, then
9 their e-mail still flows but they are not able to stop
10 people from forging messages from their domain. So, I
11 think it's something useful and can be deployed
12 incrementally.

13 MR. HUSEMAN: Ryan Hamlin from Microsoft, the
14 second part of yours and AOL's and Yahoo's proposal was
15 eliminating the ability to create fraudulent e-mail
16 accounts in bulk. Is that the limitation of sending out
17 100 messages per day, or is this a different proposal?

18 MR. HAMLIN: Yeah, so to the earlier question
19 about raising the cost barrier, we think it's really
20 important to raise the cost barrier for Spammers to get
21 accounts. So, when there is an opportunity for a free
22 account or a nearly free account, meaning we don't get a
23 full credit card and we're charging, you know, a full-
24 access fee, we want to put a barrier in place so that
25 they can't automatically -- Spammer can't automatically

1 generate mass accounts in bulk.

2 So, a few months ago, you could go out to
3 Hotmail and it was free accounts and you could have
4 automation to create thousands of accounts at a time.
5 We've since put something we call HIP, or human
6 interactive proof, in there, in the sign-up, so that when
7 you sign up, it gives basically a set of letter
8 combinations that are not readable by the machine, that
9 requires a human to put in exactly what that is, and then
10 respond, and the create is actually -- the account is
11 actually created.

12 So, we've seen a drastic account of the bulk
13 creation, once we put something like that in, so it's
14 saying where there is a low cost to barrier for mass bulk
15 accounts, we need to put a mechanism in place to stop
16 that. That's just one approach that we put in as an
17 example at Hotmail.

18 MR. HUSEMAN: Steve Atkins, what do you think
19 of that approach? Is that effective?

20 MR. ATKINS: Yeah, there's been a number of
21 cases for, oh, years back, where free web mail providers
22 have been abused by bots in this way, and the approach
23 Microsoft is suggesting is a well-proved, good one.

24 MR. HUSEMAN: John Levine, any thoughts?

25 MR. LEVINE: I agree that it's a well-proved

1 scheme, and if I may tweak you a little, Microsoft was a
2 little behind the curve on this one.

3 **(Laughter).**

4 MR. LEVINE: Honestly, I think that something
5 that's outside the purview of this panel, but what we
6 really need is a credit bureau for ISPs, so that when you
7 have someone who's been kicked off one ISP, it's harder
8 for him to sign up on another one, you know, which is,
9 you know, a completely non-technical thing, you know,
10 it's what credit bureaus do. And the world desperately
11 needs one specifically to meet the needs of ISPs.

12 MR. HUSEMAN: Microsoft, do you support the
13 creation of such a bureau of information sharing between
14 ISPs of Spammers who have been kicked off?

15 MR. HAMLIN: Yeah, in fact, I think the next
16 bullet point in the press release talks specifically
17 about that, about sharing that information. So, you
18 know, the great thing that I thought about the
19 announcement was, although, you know, Microsoft, AOL and
20 Yahoo are fierce competitors and will continue to be
21 fierce competitors, we do have one foe, and it's the
22 Spammer.

23 And, so, you know, over the months of us
24 talking, we realized that there are some best practices
25 we can share, so things like that, where we've identified

1 a Spammer on our network, there's no reason why we
2 shouldn't be sharing that with the other ISPs to take
3 advantage of that, because it is solvable by an industry,
4 because what's happening is the Spammer just hops to the
5 next network.

6 MR. HUSEMAN: So, what type of information will
7 you share?

8 MR. HAMLIN: So, there's a lot of -- there's
9 kind of two different ways. One is sharing where we
10 identify, obviously, harvest attacks or fraudulent
11 account creation via an IP. So, we potentially will be
12 discussing ways amongst the ISPs to share that
13 information. Again, we're not going to -- because of the
14 issues around blacklists, so you have to be very careful
15 there when you start sharing IPs.

16 The other area that we talked about is in the
17 area of enforcement, where we start to share electronic
18 evidence, and that kind of goes into the fourth point,
19 but it's where the ISPs work together to provide an
20 electronic record, and so instead of just a Microsoft
21 going after a particular Spammer, it's really the
22 industry of ISPs going after these folks and providing up
23 information across all ISPs.

24 MR. HUSEMAN: What type of electronic
25 information does the proposal anticipate you sharing?

1 MR. HAMLIN: So, you've got to be aware,
2 obviously, of the privacy information, but the idea would
3 be we would start to log some of the activities. So, as
4 there would be suspicious or fraudulent type behavior, we
5 could notify the ISP community and others that have
6 witnessed that same type of behavior, maybe associated
7 with a given IP could start to track some of that
8 information and logging. It doesn't mean black list
9 them, it just means track that, so if it does turn out to
10 be something of fraudulent behavior, we have that record.

11 MR. HUSEMAN: And when will that -- this take
12 place? What is your time table for implementation of
13 this?

14 MR. HAMLIN: So, I'm going to sound a little
15 bit of a broken record, but really what we want to do is
16 get the feedback from others, because we know, again, the
17 three of us alone can't solve this thing, so we need to
18 understand the technical implications across the board
19 for small ISPs to do this, for medium-sized and the large
20 ISPs.

21 MR. HUSEMAN: And, so, when are you going to
22 get the feedback from others?

23 **(Laughter).**

24 MR. HAMLIN: So, it's a great -- so the plan is
25 to absolutely in the very near short-term --

1 MR. HUSEMAN: Such as?

2 (Laughter).

3 MR. HAMLIN: I should have known with a lawyer.

4 (Laughter).

5 MR. HAMLIN: So, our plan is within the next
6 couple of weeks, we will have another discussion, the
7 initial ISPs that I talked, and then within a very short
8 time after that, let's say, you know, 30, 60 days, we'll
9 get together as an -- and invite the broader community to
10 participate. So, this is something that will get done in
11 the next couple of months, not something that's going to
12 get done in 12 months from now.

13 MR. HUSEMAN: And will this -- these
14 discussions and feedback, will that also include the
15 credit bureau/Spamming bureau sharing of information?
16 About people who have been kicked off? Will that be part
17 of this discussion that you're talking about?

18 MR. HAMLIN: Oh, yeah, all these four pillars
19 that we kind of laid out in the press release, those will
20 all be discussed at that type of a forum. And we will --
21 you know, we'll take a look at identity crisis, and we'll
22 propose the idea that we talked about already. We'll
23 look at other ideas, too, though, you know, that Paul is
24 looking at, and others in the industry.

25 But the key is, and I said it before, we have

1 to show movement. It's an incremental process, but we've
2 got to show movement. And this is a great forum over the
3 last, you know, couple of days, to just do that, get in a
4 lot of really good feedback. We now are ready in a
5 position to move.

6 MR. HUSEMAN: Steve Atkins, what would you say
7 to Microsoft about this?

8 MR. ATKINS: It's a very good idea.

9 **(Laughter).**

10 MR. HUSEMAN: Paul Judge, what would you say to
11 Microsoft about this?

12 DR. JUDGE: I will be talking to Ryan further
13 about this. We had some initial conversations. Also,
14 I'm going to talk to another group that represents a
15 different set of constituents in this ecosystem, and they
16 have a detailed proposal coming out in a few weeks that
17 looks at just that, a reputation system. I think it's
18 really a good move from black lists, which used to give
19 us a binary decision, to something like a reputation
20 system that gives us more detailed information about a
21 sender, about the bulk of mail that they send, about the
22 number of complaints that they have, and then we're able
23 to make more granular decisions about that sender.

24 MR. HUSEMAN: David Berlind, I want to move to
25 you now. You are the founder of something called

1 JamSpam. This is a consortium that you put together of
2 various industry and various other representative groups
3 to try to come up with a solution. Can you briefly tell
4 us about this group and what are your specific proposals
5 and the time frame.

6 MR. BERLIND: Thanks, Brian. First, I think
7 that Commissioner Swindle gave me the ultimate lob that
8 anybody could ever dream of this morning when he said
9 that it's up to everybody in this room to work together
10 to arrive at a solution, and there is no one particular
11 solution, so whether it's a technological solution or a
12 legislative solution, none of them will work well if
13 they're not harmonized to work together. It's sort of
14 like getting the different federal agencies to work
15 together to prevent terrorism, if they don't work
16 together, the dragnet will never be sufficiently closed
17 to keep terrorists from slipping through.

18 There are six distinct communities that must
19 work together in order for any solution, any one
20 particular solution, to work in concert with the others.
21 One of those is the ISPs and in-box providers; the other
22 one is the e-mail client and server providers; a third is
23 the e-mail security and management providers. These are
24 people who make products that run in parallel to the e-
25 mail client and servers.

1 Then there are the high-volume e-mailers, the
2 ones who are often accused of Spamming and maybe are not
3 Spammers. I'm not here to pass judgment. Then there's a
4 group of organizations that I refer to as the non-
5 commercial and non-profit privacy and anti-Spam advocacy
6 groups. And then finally the end-users.

7 All of these proposals, if each of these
8 communities goes off and works on their solutions on
9 their own, without consulting with the other communities,
10 it runs a risk of creating a solution that will undermine
11 the solution another community is working on. I'd like
12 to just say that to the extent that Microsoft, AOL and
13 Yahoo are soliciting input from the rest of these
14 communities, JamSpam is to this day the only forum and
15 it's the only one where all of those communities have so
16 far gathered to discuss the problem. And that's what
17 JamSpam is about. It's about all of these communities
18 figuring out a way to work together.

19 And just by a show of hands, so everybody's
20 really clear on the type of participation we're talking
21 about, we have leaders from every one of these sectors,
22 by the way, including AOL, Yahoo, Earthlink, Microsoft.
23 In fact, I saw them all exchanging cards for the first
24 time at the JamSpam meeting. I'd like to think that
25 that's how this collaboration came to be.

1 But could everybody in the room who is some way
2 related to JamSpam, attended a meeting or something like
3 that, raise their hands.

4 So, there's quite a few people in this room and
5 they represent all the different -- Paul Judge, you
6 didn't raise your hand.

7 **(Laughter).**

8 MR. BERLIND: Vince, did you raise your hand?

9 MR. HUSEMAN: Okay, David Berlind, so what is
10 the specific outcome of JamSpam? What is your goal?

11 MR. BERLIND: Well, the goal is that knowing
12 full well that something like the IETF has to produce a
13 protocol or enhance the protocol, as Steve said, and I
14 think I absolutely agree with that, we need a hardening
15 of the protocols. The hardening of those protocols
16 shouldn't be done without consultation from each of these
17 communities, so that we understand what the impact of any
18 hardening is.

19 To the extent that legislation is being
20 proposed, legislation shouldn't take place without
21 consulting with the technical community to see whether it
22 makes sense. I mean, it makes no sense, for example, to
23 enforce laws in different states if you have no -- if the
24 e-mail technology is blind to the geographic location of
25 the sender and the recipient.

1 MR. HUSEMAN: Let me interrupt for a minute.
2 Does JamSpam hope to introduce a specific technical
3 protocol or technical solution as a result of group
4 discussions?

5 MR. BERLIND: I think that early that was the
6 goal of JamSpam, was to create a new protocol. When we
7 suddenly realized that there are existing intellectual
8 property organizations already in place that are capable
9 of doing that. The goal switched to being one that
10 develops a 360-degree view of the complete problem that
11 all of these communities then can work off of as a
12 unified front in harmony with each other.

13 Right now, each of the communities is working
14 off of roughly a 270-degree view of the problem. And if
15 they only address those 270-degree views, then what ends
16 up happening is some part of the problem is ignored and
17 two solutions from different communities end up stepping
18 on each other. Blacklists is a perfect example.

19 MR. HUSEMAN: Well, what is your time frame for
20 the JamSpam for whatever proposals or discussions?

21 MR. BERLIND: Well, so far, we've had two
22 meetings. The first was in February, and the second was
23 in March. And last I heard, America Online volunteered
24 to host the third of these meetings. The second meeting
25 produced the 360-degree view. The third meeting is to,

1 technically speaking, to produce sort of a charter for
2 the organization, how it will work with organizations
3 like the IETF, government bodies, a variety of different
4 organizations to move the ball forward in a way that
5 again all the parts are moving in harmony with each
6 other, not going off in separate directions doing their
7 own thing.

8 MR. HUSEMAN: So, you don't have a specific
9 time frame for any end-product or resolution of this, or
10 is this more an ongoing discussion?

11 MR. BERLIND: I think it's an ongoing
12 discussion. I think that the number one priority,
13 though, just to comment on what some of the other
14 panelists have said is that one of the reasons a lot of
15 different things don't work is that there's no critical
16 mass. The only thing that's going to achieve critical
17 mass is a standard that's in place that's complied with
18 by every system that's out there.

19 And, so, the number one priority for JamSpam is
20 to make sure that such a standard is created and put in
21 place as quickly as possible.

22 MR. HUSEMAN: And, Paul Judge, you are with the
23 Internet Research Task Force, Anti-Spam Research Working
24 Group. Did I get that right? That's a lot of words.

25 DR. JUDGE: Correct, yes.

1 MR. HUSEMAN: Briefly, what is the Internet
2 Research Task Force and what is your working group?

3 DR. JUDGE: The Internet Research Task Force is
4 the -- well, it's just an organization of the Internet
5 Engineering Task Force, the IETF, that standardizes many
6 protocols, the body that standardized SMTP and HTTP and
7 so on. The Research Task Force has historically
8 consisted of just a small number of groups focused on
9 problems that are important to the future of the
10 internet.

11 And we formed the Anti-Spam Research Group to
12 focus on just that, the problem of unwanted messages and
13 from the viewpoint of a networking problem and seeing how
14 it's affecting local networks and internet and so forth.
15 When we chartered the group a few months ago, we charted
16 it realizing that the definition of Spam is really
17 inconsistent and not clear, so we generalized the problem
18 into one of constant base communications, meaning that an
19 individual or an organization should be able to define
20 either consent or lack of consent from certain types of
21 communication. So, from there, our goal is to first
22 understand the problem, collectively propose solutions
23 and then evaluate those solutions.

24 MR. HUSEMAN: So, what authority or incentive
25 is there with the IRTF, for whatever proposals you come

1 up with for the internet community at large to adopt.

2 DR. JUDGE: So, I believe, in general we're
3 dealing with the Spam problem, it's not hard to motivate
4 the problem. So, I don't believe that we need to provide
5 much incentive for people to do the work. The research
6 group really provides a forum for people to come together
7 to collaborate on a common ground. I think previously
8 that there's been many individuals interested in the
9 problem, and we've been in different corners of the world
10 working on the problem. And we began to have meetings
11 like this and on the research group meeting, only in
12 January of this year that this group of people began to
13 come in the same room. So, through the research group,
14 our goal is to bring these people together and have some
15 collaboration on the problem.

16 MR. HUSEMAN: So, your group will possibly come
17 up with new protocols?

18 DR. JUDGE: So, a number of things, as I
19 mentioned. It's really three phases. One is to
20 understand the problem. The second is to propose and
21 collect proposals for solutions. And then to evaluate
22 those proposals. And as far as understanding the
23 problem, I believe that we know a lot about the size and
24 the growth of Spam, but there's many characteristics of
25 the problem that we don't understand as a community.

1 Traditionally, any problems in networking and security,
2 there's a lot of effort to characterize that problem and
3 to understand and allow trace data to be established so
4 that we can study exactly where we need to focus. And
5 that hasn't been done traditionally. We've taken more ad
6 hoc approaches to the Spam problem. So, we're really
7 trying to take a more systematic or research-oriented
8 approach to it.

9 And the second piece, as I mentioned, was
10 either proposing solutions or first of all collecting the
11 solutions that have already been proposed. So, one thing
12 that we did that was very important was to establish a
13 complete taxonomy of all the solutions that have been
14 proposed over the years and to begin to understand how
15 those interrelate and how they can be put together to
16 leverage the benefits of each other.

17 And the third piece, as I mentioned, was
18 evaluation. And I think over the years, that solutions
19 have been proposed and persons have gone out and deployed
20 those solutions, and it wasn't a lot of thought put into
21 the evaluation, not only of the effectiveness and
22 accuracy but also the burden of introducing this and how
23 robust the solution is to countermeasures, and that's how
24 we got ourselves into the cat-and-mouse game that we're
25 into.

1 So, as we think through the solutions now,
2 we're able to make better decisions, and objective ones,
3 about the solutions that we propose and move forward
4 with.

5 MR. HUSEMAN: What is your time frame for your
6 Research Working Group?

7 DR. JUDGE: So, the group was chartered a few
8 months ago. We had the first physical meeting in San
9 Francisco in March. We had about 250 participants there.
10 Most of the work is done through interactions on the
11 mailing list and off-line. And there's a number of work
12 items that have been identified and we're currently
13 working on. And there's a range of things, though,
14 everything from the taxonomy to really working on
15 measurement and analysis work.

16 And there's a lot of collaboration between
17 different companies, ISPs, also different interest groups
18 and whatnot. For example, at the first meeting, as we
19 talked about the collaboration of the different
20 constituents, we had representatives from each of those
21 organizations, and many of the persons I assume that are
22 in this room, were working on different projects. So, I
23 can get into the details of each one of these, but things
24 are ongoing as we speak.

25 MR. HUSEMAN: So, when do you see the process

1 being completed?

2 DR. JUDGE: I don't know, when have we solved a
3 problem? Is it when --

4 MR. HUSEMAN: Are you talking about months, are
5 you talking about years from now?

6 DR. JUDGE: I think that -- you said the
7 process being complete, as far as the work of the
8 research group?

9 MR. HUSEMAN: Yes.

10 DR. JUDGE: Something that's -- there's short-
11 term deliverables as well as medium to long-term
12 deliverables. And some of the short-term ones are the
13 analysis and the taxonomy work. And then there's some
14 short-term to medium-term actual solutions that we can
15 roll out, mainly the identification systems, things such
16 as reverse MX and the reputation systems that we talk
17 about, introducing authentication and accountability into
18 the system are short to medium-term, so you know, six to
19 12 months we can begin to roll some of these out
20 incremental.

21 And then from there, there are more long-term
22 things that we want to do, as we chartered it with this
23 view of a consent-based communications framework, that's
24 something that's definitely more long-term, allowing us
25 to have granular definitions of different types of

1 messages and be able to enforce that policy. So, you
2 know, to get to a perfect system, it's a few years, but
3 to significantly affect the problem, it's more short-term
4 than that.

5 MR. HUSEMAN: John Levine, what are your
6 thoughts on the IRTF's working group efforts? Are you
7 involved in this group, by the way?

8 MR. LEVINE: I stopped reading their mailing
9 list a couple of months ago, so I don't really know what
10 they're doing now.

11 MR. HUSEMAN: And is there a reason you stopped
12 reading their mailing list?

13 MR. LEVINE: I have to say -- I talked to Paul
14 a little bit a couple of nights ago, which is I didn't
15 get the impression that the people in this -- at least on
16 the mailing list had done their homework very well. I
17 mean, I saw a lot of suggestions coming up and saying,
18 you know, sort of suggestions that looked awfully
19 familiar and that if -- I mean, I think a taxonomy is
20 great, but I think also a taxonomy of how approaches have
21 succeeded and failed would be -- is really important. I
22 didn't see much appreciation at that point for all the
23 work that had been done and the subtlety of some of the
24 problems that people had run into.

25 MR. HUSEMAN: Paul Judge, your response?

1 DR. JUDGE: As he said, he stopped reading the
2 mailing list a few months ago. I don't believe that he's
3 looked into the details of the taxonomy or probably would
4 have had some input into the one that was presented. But
5 the point is that we have a research group and we
6 announce that we're working on Spam, and there's many
7 people across the world that are very sensitive and very
8 emotional about this problem, everyone ranging from
9 people that sit here that work on it day in and day out
10 for the last couple of years to people that are end-users
11 that want to affect the problem and believe that they
12 have a bright idea.

13 So, as this open research group, as we're
14 currently chartered, we must deal with that entire range
15 of persons, so, there is, you know, some noise on the
16 mailing list that is not the most insightful
17 contributions, but there are many work items that are
18 defined and are being worked on in the mailing list. So,
19 persons that are paying attention to the mailing list can
20 understand and appreciate that.

21 MR. HUSEMAN: Steve Atkins, will such an
22 approach be effective with so many different users
23 involved?

24 MR. ATKINS: Such an approach as the ASRG
25 mailing list or -- I'm unclear?

1 MR. HUSEMAN: As the Anti-Spam Research Working
2 Group, can this approach or such an approach like that be
3 effective with a solution?

4 MR. ATKINS: I haven't stopped reading the
5 mailing list, but apart from that, I would agree
6 completely with John.

7 MR. HUSEMAN: And why is that?

8 MR. ATKINS: The amount of traffic on the
9 mailing list was very high. Those people who actually
10 work in the industry and understand the issues and have
11 looked at the approaches three, four years ago that the
12 ASRG is revisiting or reinventing now, mostly left in the
13 first three or four weeks, because the amount of signal
14 was low and the amount of noise was high.

15 MR. HUSEMAN: Paul Judge, what is your
16 response, if you have anything in addition to add,
17 besides what you already said about this issue?

18 DR. JUDGE: Well, so this is in the first three
19 or four weeks when we really dealt with many newcomers to
20 the area of Spam. This was not the persons that are
21 sitting on this panel or many people in the room, but
22 people that really didn't know much about the problem and
23 came on to the research group looking for answers. And,
24 so, there was a significant amount of noise; however, the
25 research group isn't an entity or a body that exists by

1 itself. It's really a group of individuals, and it's
2 about individual contribution, and it provides a place
3 for people to come together and work on the problem.

4 MR. HUSEMAN: So, do you have any specific
5 proposals, or is that later on in your phase? And do you
6 have any specific things about what types of solutions
7 such as this will work, either be it protocol changes or
8 advanced filtering or et cetera?

9 DR. JUDGE: As I mentioned, there are a range
10 of things we looked at, first of all, the things that
11 have been proposed already, to sort of understand the
12 solutions base and to realize that we've almost completed
13 filling the solutions base, but as far as different
14 proposals, it's individual contribution, and if you look
15 back at the first meeting we had, there's been two major
16 approaches submitted or published this week. One was by
17 ePrivacy Group; and one was by NAI and their Lumos
18 system. And both of those proposals were presented at
19 the first Anti-Spam Research Group meeting. A few other
20 proposals and systems we see information about on the
21 table out there were presented as part of the Anti-Spam
22 Research Group. So, I believe that, you know, a number
23 of things have been funneled through there.

24 MR. HUSEMAN: So, your position is that this is
25 causing or helping with these proposals to being

1 introduced, is that correct?

2 DR. JUDGE: Yes.

3 MR. HUSEMAN: Okay. Let's talk about one of
4 the proposals that was mentioned. Vince Schiavone
5 briefly is going to talk about what he sees as a
6 structural solution or protocol change to e-mail and
7 describe that.

8 MR. SCHIAVONE: Having developed the trusted
9 sender program and deploying it last year, we agree very
10 much that there is a critical mass issue and it requires
11 support. We are at some chicken-and-egg situations as
12 far as e-mail goes. One of our large clients challenged
13 us that for anything to pick up critical mass, it really
14 needed to be an open standard that was free and available
15 to all and involved many, many people.

16 What we heard here today so far is that we've
17 been putting a lot of band-aids on something and we're
18 losing. I mean, all these technologies are getting
19 better and better and better, yet Spam is increasing
20 geometrically in my e-mail box and in the filters before
21 it gets to me. What Commissioner Swindle said this
22 morning is we need to give the ISPs and the consumers a
23 way to decide who and what they want to receive. Well,
24 the who and what is the problem. Foundationally and
25 fundamentally, there is no trust in e-mail. It was never

1 meant to contain trust, and I don't know who's sending me
2 e-mail.

3 What I'm receiving, there's no standard way for
4 NAI members to tell me I'm receiving a statement, so my
5 filter people don't inadvertently block it. So, what
6 we've done is proposed here today an open standard where
7 we are willing to contribute our technology and hope
8 others will stand up to contribute theirs, to try to get
9 to the point, using today's existing standards to
10 seriously separate the good e-mail from the bad e-mail.
11 And I'll go through it very quickly, or Brian will kick
12 me off, he said.

13 **(Laughter).**

14 MR. SCHIAVONE: And at 4:00 in the afternoon,
15 that's very sensitive.

16 What we've learned in the last few years is how
17 not to fix e-mail. Technology can only enforce policy;
18 it can't create it. It can't tell who it is. Policy
19 that's not aligned with technology won't work either,
20 because it can exclude a lot of different people. An
21 important thing that you'll hear us say is the ISPs
22 adopting standards or not adopting standards is the issue
23 that will change how Spam occurs, because so many -- so
24 much of the e-mail goes through them.

25 How to fix ISPs, we feel, is to use the ISPs

1 and the laws to encourage both a carrot and a stick
2 approach. The ISPs can block things, okay? But they can
3 also encourage, not give a free pass, but to weigh
4 positive features that people step up to. The laws can
5 create penalties, but they can also create safe harbors
6 for people who choose to do things that encourages good
7 behavior.

8 Our standard that we're proposing is a
9 framework to provide trusted identity. The commerce on
10 the web today is based on the DNS system with digital
11 certificates layered on top of it, because DNS is not
12 secure. We don't know who's sending. There's spoofing
13 because there is no security, so we have to add it. We
14 need to know with a secure, fast and lightweight method
15 who is actually sending us e-mail, making trusted
16 assertions. We need to know who the sender is, and we
17 should have the ability for them to communicate to us the
18 content of the individual e-mail, and many people in this
19 group, although they may not agree what the permission
20 should be, might think it would be useful that the
21 permission be communicated with the e-mail. We need to
22 create a framework for creating a federation of trusted
23 e-mail programs. JamSpam was a great way to get
24 everybody together, and it's only through cooperation and
25 harnessing all the energy in this room that we get there.

1 Our plan calls for a small oversight board,
2 very representative of the 360-degree view, okay? Oops,
3 I'm on timing. Did you add the timing to this, Brian?

4 We believe there needs to be very minimum
5 standards that do not disenfranchise either anonymous
6 individual e-mail, which is very important to the
7 internet, as well as small businesses who should not have
8 to bear high costs. And that should include a basic
9 identity, near zero costs, but create a standard language
10 for stating it and communicating.

11 We also suggest a standard language for stating
12 assertions, but at this level, it should be optional.
13 It's very sensitive, excuse me. Is it unsolicited e-
14 mail? Is it permission-based? We're not advocating
15 labeling in the subject line. Mail moves very quickly
16 and in large volumes, and if we want to empower ISPs and
17 consumers, there need to be electronic ways for them to
18 see, sort and decide what they wish to do to the e-mail.

19 Now, the bulk senders, the NAI e-mail service
20 providers, deserve a lot of credit for the Lumos
21 proposal. It's a very high standard they're talking
22 about. They're talking about identifying themselves when
23 they send e-mail at a secure level with a digital
24 signature, as well as DNS, and asserting what type of e-
25 mail it is. That is a very, very good plan.

1 Additionally, they may want to do a relationship
2 permission. At this level, we should know who the people
3 are and there should be a cost to that so it can start to
4 change the economics of Spam, who are the people who are
5 sending e-mail? And it's very important that there be a
6 standardized opt-out. We're hearing from our friends at
7 the filter companies and the ISPs, and these are things
8 that can happen today.

9 At the highest level, if things that would
10 create a visible seal for the consumer, and that's where
11 our trusted sender program plays, there needs to be very,
12 very sure ID. And visible assertions that should be made
13 that there is a way to opt out that can be trusted, that
14 there is a link to a privacy policy, that there is a
15 dispute resolution mechanism in force. A trusted sender
16 is with TrustE, which is a good body for industry self-
17 regulation.

18 And the last thing I want to say, with this
19 program that's an open standard and involves many, we can
20 do this without breaking the existing protocols or
21 waiting -- Paul's work is very important at the ASRG, but
22 it takes time to change protocols at that level. We have
23 existing protocols for SMTP with X headers, and we have
24 existing protocols with X509 certificates that can change
25 this problem very quickly.

1 I just wanted to let you in on some information
2 we know. There's an ROI for trust. We have done some
3 studies with the program. We cannot name it, but there
4 are higher open rates. There are higher click-through
5 rates and there are lower opt-out rates. But more
6 importantly, look at the numbers for the trust ROI.
7 Trust pays for people, and as Commissioner Swindle said
8 earlier today, we need to do something that will
9 fundamentally change this equation in the short time.
10 Steps that don't go from the legal responsible sender,
11 okay, to the actual recipient and their ISP, with
12 confidence in who they are and what they're sending, are
13 only half steps. The mailers are very -- the service
14 providers are willing to go there, and the advocates who
15 supported this plan this morning, and we thank them, are
16 willing to be part of this as well.

17 So, that is our pitch for this. This is not an
18 exclusion to anything that's happening here, but it's the
19 first step where we come together and make technology a
20 royalty-free open standard to enable all this to happen.
21 Thank you.

22 **(Applause).**

23 MR. HUSEMAN: John Levine, your thoughts on
24 this proposal?

25 MR. LEVINE: I've actually looked at in some

1 detail, because the CAUCE board -- I'm a member of the
2 board of CAUCE, and we have endorsed the concept, not the
3 product or the implementation or anything, but the
4 concept of being able to put assertions on e-mail like
5 this that you can test and you can actually determine
6 whether a mail purports to be bulk or doesn't purport to
7 be bulk and who is making the assertion.

8 And although, like nothing else, it's no magic
9 bullet. I was actually surprised. It looks really good.

10 MR. SCHIAVONE: Yeah, how about that?

11 **(Laughter).**

12 MR. LEVINE: And I think that something like
13 this that can be layered on top of mail and particularly
14 could work with laws that could -- assertions in mail
15 about what the mail is, if it were -- that would make it
16 easier to enforce laws that could sanction you if these
17 statements you made about the mail you sent weren't true.

18 MR. HUSEMAN: David Berlind, do you have a
19 comment on this proposal?

20 MR. BERLIND: Yeah, I think that -- first of
21 all, I want to commend every organization that steps
22 forward and says certify us, give us a hall pass based on
23 our -- some best practices that we've advanced. But you
24 should be aware of the fact that there are probably 20
25 such organizations, all who have advanced a separate set

1 of best practices. There's no uniformed set of these,
2 and that any time I hear the words dispute resolution,
3 first of all, I -- you know, as a technologist, I say
4 that's a human process, it's not possibly scalable on a
5 global basis, number one; and number two, it implies a
6 great degree of subjectivity.

7 And, so, you know, I think to the point of
8 things like attestable things, like a verifiable -- I saw
9 it in the diagram -- a verifiable opt-out link, that
10 there should be no one set of best practices that speaks
11 on behalf of me and what I want in my inbox. In fact,
12 these best practices are proposed by the organizations
13 who represent a high-volume e-mail constituency. They
14 never consulted with me. And, so, it's kind of like the
15 fox watching the hen house.

16 I think that ultimately what I want is a set of
17 things that can be tested, like an unsubscribe link, that
18 I can say well, if the e-mail has an unsubscribe link or
19 something that terminates my relationship and it
20 functions, then go ahead and let it through, but if it
21 doesn't, then don't let it through. But I worry about
22 any system that's based on best practices when currently
23 we have no agreement on best practices within the borders
24 of the United States and we certainly will never get an
25 agreement internationally.

1 MR. HUSEMAN: Vince Schiavone, your response?

2 MR. SCHIAVONE: That's why we suggested there
3 be an open standard of the ability to make assertions
4 that will vary, because David's absolutely right, it's up
5 to him what he wants to accept, and it's up to the ISP
6 and their acceptable use policy. But if we have a
7 standard way to make these assertions, then they can
8 happen in a scalable way. And one other quick thing I'd
9 like to say, we do have experience that with e-mail, much
10 of dispute resolution, a very, very high percent of it,
11 is automatic, it can be handled electronically, because
12 mostly people want to come off the list, and they want to
13 know that that will actually happen.

14 MR. HUSEMAN: Steve Atkins, any thoughts on
15 this proposal?

16 MR. ATKINS: Of the various trust proposals
17 I've seen, it's one of the better fleshed out. I'm not
18 entirely convinced that trusted sender is the answer to
19 everything, but it is a good way of reducing false
20 positives if it's maintained properly.

21 MR. HUSEMAN: Steve, you also have your own
22 proposal to change the protocol of e-mail. Can you
23 briefly describe what you envision as solving the Spam
24 problem.

25 MR. ATKINS: Well, watching a lot of the

1 discussions over the past couple of months, I've seen an
2 obsession with putting more and more band-aids and duct
3 tape around SMTP, and there's good reason for that.
4 Rolling out a new protocol to replace SMTP altogether,
5 the deployment issues are horrific. It would take many,
6 many years. But that doesn't mean that it's not possible
7 to use a different protocol in addition to SMTP for some
8 of the applications that SMTP is currently used for.

9 So, I looked at some of the problems with
10 solicited bulk e-mail, newsletters from a company that
11 you've actually opted into and want to receive and saw a
12 couple of problems. One is that an awful lot of them get
13 caught in Spam filters because they look Spam as far as
14 the rules-based system are done. A properly done
15 newsletter will have an opt-out link. A very well known
16 and widely used Spam filter considers an opt-out link to
17 be a sign of Spam, so a lot of newsletter get erroneously
18 filtered, a very high fraction of false positives in Spam
19 filters are solicited bulk e-mail.

20 The other problem related with that is that the
21 recipient has lost all control. They give their e-mail
22 address to the sender, and then they have no control over
23 what happens with it. The sender can sell it on; the
24 sender can refuse to unsubscribe them when asked.
25 They're relying on the integrity of the sender to control

1 their mailbox.

2 Because of that, they often fear to sign up for
3 them. They're wary of signing up for newsletters,
4 because they don't know what will happen when they do.
5 They don't know whether they'll be able to unsubscribe,
6 so I've spent the past few days fleshing out a short
7 discussion document for an alternative protocol that
8 you'd run in parallel with SMTP that any sender could
9 choose to use in addition to their bulk mail
10 distribution; any recipient could choose to use in place
11 of their normal mail client or as part of their normal
12 mail client, whereby instead of them sending their e-mail
13 to address to the sender of the newsletter and the sender
14 then starts sending it, instead the recipient fetches the
15 newsletter from the publisher, and that way they have all
16 control over when it's sent and when it isn't sent, and
17 if they're subscribed to 20 different newsletters from 20
18 different publishers, they're all administered in the
19 same way, from a single screen on a single client. The
20 full details are pretty simple.

21 It's the sort of protocol which could be
22 prototyped in a couple of days. It could be made, you
23 know, deployable within a month or so. If anyone's
24 interested to talking about it, it's available up on my
25 website at word-to-the-wise.com. And there's a dozen or

1 so copies on the table outside.

2 MR. HUSEMAN: Ryan Hamlin from Microsoft, what
3 are the practical difficulties of any protocol change,
4 such as the one Steve Atkins just described?

5 MR. HAMLIN: So, I don't -- you know, specific
6 to Steve's -- I would love to look at it. I haven't had
7 a chance to really look at. I think that Steve said it
8 right, I mean, the implementation -- there's a lot --
9 there's a lot of really good proposals, and Vince's is
10 one and NAI's Project Lumos is yet another. The devil's
11 kind of in the details in really understanding how long
12 it's going to take to roll this out.

13 I'm a strong believer in an incremental
14 approach and that we are going to learn in kind of a
15 trial by error, so taking the approach of something and
16 trying it and seeing if it makes an effect, what kind of
17 an effect it does have and if it does, roll it out
18 broader, and then going back, and not trying to build,
19 obviously the one-all solution today.

20 MR. HUSEMAN: John Levine, your thoughts on the
21 practical realities or difficulties of any protocol
22 changes?

23 MR. LEVINE: Getting rid of SMTP isn't going to
24 happen for decades, if ever. But Steve is absolutely
25 right, that for certain kinds of transactions, there are

1 other alternatives. I mean, mail is fundamentally a
2 rotten way to send the same message to a million people.
3 You're much better off doing that with -- over the web.
4 You know, and if you can sort of remind the million
5 people that here is a URL to go to to look at your
6 newsletter, that's much -- you could concoct a scheme
7 that would be much more resistant to abuse. You would
8 waste much less bandwidth, because people would actually
9 fetch the text of the newsletter when they were prepared
10 to read it. And you could run something like that in
11 parallel with e-mail.

12 You could tell people like here's your
13 newsletter toolbar, which is automatically set up to kind
14 of light up the buttons when there's a new issue ready to
15 look at. And Steve is absolutely right, that sort of
16 thing can be built on top of existing alphabet soup
17 things like XML very quickly and could be quite useful as
18 a way both to manage your subscriptions and to push back
19 a whole bunch of Spam-like issues.

20 MR. HUSEMAN: David Berlind.

21 MR. BERLIND: Well, one thing about just that
22 particular proposal is that e-mail is by nature a store
23 and forward technology. There are millions of people who
24 download their e-mail to their system and then read it
25 later on an airplane. And, so, if I got some sort of

1 stub of an e-mail that said okay, now, if you want to
2 read this newsletter fetch it, but I'm on an airplane
3 where I can't get it, that would be problematic. There
4 are probably ways around that, but that would be
5 something that has to be addressed.

6 I absolutely agree that this has to be
7 addressed at a protocol level. And I'll just give you
8 another suggestion or another idea that happens at the
9 protocol level, which is to take the notion of opt-out
10 links completely out of the control of people who send e-
11 mail to me or anybody else and build it into the
12 protocol. Unsubscribe really means terminate
13 relationship. The protocol right now, you know, in your
14 e-mail client, you know, you have a send button, you have
15 a reply button, why not a terminate relationship button?
16 And when the e-mail arrives into my inbox, my inbox goes
17 to check to see if the sending system will correctly
18 respond to that command, and if it will not respond to
19 that command, then it doesn't let the e-mail through to
20 me.

21 It also provides an interesting test for
22 legislators to say, hey, have you disabled this part of
23 the protocol, it's kind of like disabling your odometer,
24 you broke the law. Okay, that part of the protocol
25 cannot be disabled, you have to respond to a terminate

1 relationship command.

2 And, so, I think there are plenty of really
3 interesting things that can be done at the protocol level
4 that serve as a pass-fail way of not eliminating the Spam
5 problem from a technological solution but also from a
6 legislation solution.

7 MR. HUSEMAN: I'm going to open the floor to
8 questions now. This gentleman over here. Wait for the
9 microphone, please.

10 MR. ROYSTON: Clifton Royston, LavaNet. I
11 think we've just seen a great demonstration of why it's
12 hard for the ASRG to make progress, because what Paul
13 Judge, to his great credit, is doing has been managing
14 for the last three months or so, more actually,
15 succession of really clever, intelligent ideas like this
16 from many very bright people, proposals like we've just
17 seen from Vince, Ryan, Steve, David, about every three
18 hours over the period of the last three months, there's a
19 lot of good ideas out there, and I -- to be honest, I
20 think some of the grilling that was directed at Paul
21 Judge representing the ASRG in the context of how many
22 weeks from now are you going to give us a solution to
23 Spam, reflect a misunderstanding of what -- not only how
24 the IETF works but what the distinction is, which is
25 going to make no sense to many people who are between the

1 IETF -- Internet Engineering Task Force and a research
2 task force. I understand all these issues that keep
3 getting raised with each proposal that comes up is this
4 going to work a year down the road, two years down the
5 road? What will this break? Paul has been tasked with
6 making sure that what gets proposed is good for the next
7 20 years once it's deployed and that's --

8 MR. HUSEMAN: So, your point is that there are
9 great difficulties in coming up with these solutions and
10 that the process of sorting through all these ideas is
11 difficult, which I guess leads me to a question of all
12 the panelists. Will any -- will there be any
13 technological solution or structural change to e-mail
14 that will stop Spam?

15 MR. BERLIND: I would say the answer to that is
16 the day that everybody decides to work together, and I
17 mean the six different communities, we'll have a solution
18 on very short order, as long as they commit to that.

19 MR. HUSEMAN: Let's keep it brief. Vince
20 Schiavone?

21 MR. SCHIAVONE: Absolutely. As soon as we add
22 security and trust to e-mail, we can get to the solution
23 that excludes it. It will always come in, but it will be
24 treated much differently than trusted e-mail.

25 MR. HUSEMAN: John?

1 MR. LEVINE: Will there be changes? I think
2 the answer is yes, because when the three big gorillas --
3 you know and say that, you know, you have to play by our
4 rules to send us mail, the rest of us will have to do
5 what they say. And it -- that's true, but it remains to
6 be seen whether it's Vince's proposal or something else,
7 whether it will actually deal with the issue in ways that
8 Spammers can't get around.

9 MR. HUSEMAN: Ryan Hamlin?

10 MR. HAMLIN: Not as concerned as much about the
11 forum, I think everyone has to have a seat at the table,
12 which we will drive forward with. As an industry now
13 it's very apparent, as well as being, I guess, one of the
14 gorillas, I would say it's -- you know, we have high
15 incentives to solve this problem. Not only is it the
16 number one concern our consumers have, it is costing us
17 millions of dollars a year to do that. So we are highly
18 incentive to move forward on these.

19 MR. HUSEMAN: Matt Sarrel?

20 MR. SARREL: There will eventually be a
21 solution. I think that, you know, in very vague, very
22 quick terms, it will rely on knowing who the -- an
23 authenticated sender, an unmodified e-mail that clearly
24 states what it is and the recipient having an easy and
25 accurate way of opting out.

1 MR. HUSEMAN: Dan Tynan?

2 MR. TYNAN: If you're speaking purely as a
3 technological solution, then, no. Technology in
4 combination with some form of, hopefully, smart
5 legislation and perhaps private right of action combined
6 may do it. But just providing technology will not get
7 rid of the bad actors.

8 MR. HUSEMAN: Paul Judge?

9 DR. JUDGE: It's a simile with Daniel, that the
10 solution is definitely one that's technical and
11 legislative and so on, but on the technical side, I have
12 not seen a silver bullet. I believe I've seen, you know,
13 every proposal for anti-Spam system, but I haven't seen a
14 silver bullet. I've seen a number of systems that
15 crafted together carefully will tremendously help us to
16 control the problem, and I think again it's about
17 collaboration, people deciding that we're going to work
18 together and come to some consensus and work together to
19 deploy this.

20 MR. HUSEMAN: And one point of clarification
21 about the process, correct me if I'm wrong, but your
22 Anti-Spam Research Working Group will then make
23 recommendations to your Internet Research Task Force,
24 which is a sister organization of the Internet
25 Engineering Task Force, which will -- is then the

1 organization that sets the standards for the internet.

2 Is that correct?

3 DR. JUDGE: So that's -- that's correct, one
4 form of deliverables is recommendations on a solution set
5 and that could be made as recommendations to the IETF,
6 but in reality, there's really a couple of paths to
7 solving a problem, and one is that traditional
8 standardization approach. And that does take some time.
9 But there's also de facto standards, they're sitting down
10 and writing code and, I mean, code talks, and we're not
11 confused about that, so that's why we're forging
12 relationships between -- for example, in the Spam
13 research group, every company that creates an anti-Spam
14 product participates in that group. So, if you have
15 consensus among that group and you begin to have
16 consensus between those groups and the ISPs, then we can
17 have things that are out there and out there working in
18 the short term.

19 MR. HUSEMAN: Steve Atkins, to get back to the
20 question, will there -- or is it possible to have a
21 structural solution or technological solution to Spam?

22 MR. ATKINS: I don't believe a purely
23 technological solution is possible, because as several
24 people have mentioned, SMTP is not going to go away. For
25 decades there will be people who will want to send my e-

1 mail over SMTP, so there will have to be some way for
2 them to talk to me, even if I'm primarily using a
3 different protocol. But I believe a combination of
4 technological fixes and possibly legislation and
5 definitely a lot of social and communication work,
6 primarily between ISPs will happen, and it will happen
7 soon. And the reason I say that is if it doesn't happen
8 soon, in a lot of areas, SMTP mail is going to fall over
9 or get worse. Even filters just push the problem to the
10 ISPs, rather than the recipients. So, yes, there's going
11 to be a technological and social fix soon, because
12 otherwise everything is going to break.

13 MR. HUSEMAN: One question I had before I turn
14 it back to the audience. We talked legislatively about a
15 do-not-Spam list. Is such a list currently
16 technologically feasible?

17 MR. LEVINE: I actually talked to Senator
18 Schumer's office about this yesterday. A list of e-mail
19 addresses is not practical. It would be too huge and too
20 impossible to maintain and too onerous. As I said to
21 them, I mean, do you really expect General Electric and
22 Citibank to give you a list of all of their employees, to
23 beg people not to Spam it. On the other hand, if you do
24 it at a higher level, by domain or by putting no-Spam
25 tags on mail servers, I think that would be

1 technologically implementable. As in connection with an
2 effective do-not-Spam law.

3 MR. HUSEMAN: Vince Schiavone?

4 MR. SCHIAVONE: I hope it's not inevitable, but
5 with the -- I'm from Pennsylvania, and our do-not-call
6 list was very popular very quickly. Because I think a
7 do-not-e-mail list would be a very bad idea. It's a
8 different medium, and there are people who forget when
9 they opt out that they also signed up to receive
10 information. There's a lot of confusion.

11 We do not currently have clear standard
12 definitions of what a newsletter is or what UCE is, and
13 if we need to go a step before that where we have some
14 type of classifications that people can choose to sort
15 by.

16 MR. HUSEMAN: But does the technology exist to
17 have such a list?

18 MR. SCHIAVONE: The technology exists to do
19 everything, but just like with Eileen here, if you fund
20 it enough, we can do it, but I still don't think it's a
21 good idea or it will work very well.

22 MR. HUSEMAN: Paul Judge, would a do-not-Spam
23 list be technologically feasible?

24 DR. JUDGE: Yes, we have the technology to make
25 it secure and to make it efficient. So, yes, it's

1 technically feasible. The one question is opt out of
2 what?

3 **(Laughter).**

4 DR. JUDGE: I don't think the answers
5 necessarily are global opt-out of e-mail. I think that
6 you have to get some granularity there or you have to be
7 able to express what you're expressing the lack of
8 consent for, what type of communication do I not want to
9 receive. And then perhaps there's multiple opt-out
10 lists, and then you begin to have something that's
11 useful.

12 MR. HUSEMAN: David Berlind?

13 MR. BERLIND: I think that such a list is just
14 totally impractical, and the reason is that it relies on
15 the fact that you have to define Spam, and that problem
16 will never get solved. And I think that the real answer,
17 if you're looking for some form of list management, would
18 be a permissions data base, which basically allows me to
19 track who I've given my permission to and who I have not
20 and then when somebody sends me something, it better come
21 with that permission attached to it.

22 MR. HUSEMAN: Steve Atkins, is a do-not-Spam
23 list technologically feasible?

24 MR. ATKINS: Do-not-Spam is so ill-defined that
25 no, it's not feasible. What's really meant is a list of

1 e-mail addresses or domains which do not want to receive
2 some specific type of e-mail. Let's call it unsolicited
3 bulk e-mail that is well defined. Is it technologically
4 feasible? Yes. But at that point it becomes merely a
5 legal nicety, because the last time such a list was
6 created, one of the first things that happened was the
7 whole of aol.com opted out. At that point, it's going to
8 be used purely as a pretext for legal action, rather than
9 as anything that really gives choice to the end-user,
10 because given the choice, the end-users don't want
11 unsolicited bulk e-mail, except for a very tiny fraction.

12 MR. HUSEMAN: Let's open it back to questions
13 from the audience again.

14 MR. HUGHES: So, we're on the topic of do-not-
15 e-mail lists. So, the question for the panel is doesn't
16 a do-not-e-mail list create the richest source of e-mail
17 addresses for Spammers? And doesn't the security around
18 that list become an enormous problem? It just seems to
19 me that that makes it an absolutely horrible idea.

20 MR. HUSEMAN: John Levine?

21 MR. LEVINE: You're absolutely correct, and
22 that's one of the reasons why I suggested to Senator
23 Schumer's office that doing it by domain or by server is
24 much more practical, because then you're not listing
25 individual addresses; you're only listing domains which

1 are already publicly known.

2 MR. HUSEMAN: Vince Schiavone?

3 MR. SCHIAVONE: Yes, it is a security
4 nightmare. We've heard things of a hail storm where all
5 data was stored in one particular silo. It's a very bad
6 idea. But David Berlind suggesting that permission,
7 whatever it be, whether it's unsolicited, whether it's
8 existing relationship, can go with each and every e-mail.

9 MR. HUSEMAN: Paul Judge?

10 DR. JUDGE: So, I believe, yeah, if you
11 implement it in a naive manner, then it's insecure, but
12 there's very basic technologies available to implement a
13 secure data base, simply an e-mail address and a data
14 base of hashes of e-mail addresses. You'd have a one-way
15 hash function of e-mail addresses, then you allow someone
16 to check whether or not an e-mail is in that data base or
17 not, without ever having access to what e-mail addresses
18 are in there.

19 MR. HUSEMAN: Steve Atkins?

20 MR. ATKINS: What he said.

21 **(Laughter).**

22 MR. ATKINS: An e-mail opt-out list is a bad
23 idea, but the security issues are not the reason it's a
24 bad idea. They're easily resolved.

25 MR. HUSEMAN: The gentleman in the striped

1 shirt, right there.

2 AUDIENCE MEMBER: There was a solution that was
3 mentioned at the beginning, and I don't think it was paid
4 enough attention to, maybe because it's a good solution
5 for users. I think it's also a good solution for those
6 who send permission-based e-mail, and that is a token-
7 based system, so the idea is that you take an e-mail
8 address, and we understand that now to have two parts,
9 the part before the @ sign and the part after the @ sign.
10 What we can do is put in there a token, and this already
11 exists in several ISPs. In the ISP I use, it's there.
12 So, you have the first part, a plus sign, the token, the
13 @ sign, and then the domain.

14 Now, that gives -- I think that solves the opt-
15 in problem, because you've opted in because I've given
16 you a token to get into my inbox. So, I think that's a
17 good solution for those who want permission-based
18 marketing. I think it's a good solution for users
19 because it gives them virtually unlimited number of e-
20 mail addresses that they can use, and they can filter on.

21 MR. HUSEMAN: Any comments from the panel on
22 that question? Vince Schiavone.

23 MR. SCHIAVONE: E-mail's big and fast, and
24 there's a lot of scalability issues, and disposable e-
25 mail addresses are very good for technical people like us

1 in this room, but most consumers cannot handle it.

2 MR. HUSEMAN: One more response and then one
3 more question. Steve Atkins?

4 MR. ATKINS: They're what I use, but they are
5 not really appropriate for a lot of end-users. Managing
6 the data base of them gets a little complex.

7 MR. HUSEMAN: Then Jason Catlett in the back,
8 Jennifer.

9 MR. CATLETT: Thanks, Jason Catlett from
10 JunkBusters, and I'm against Spam, and I encourage
11 filtering by ISPs, but I don't feel entirely comfortable
12 with the prospect of the three gorillas, as John Levine
13 called them, getting together and running the post
14 office, particularly when the three gorillas each have a
15 large catalog business of their own. Is there anyone
16 else who is worried about that?

17 **(Applause).**

18 MR. HUSEMAN: John Levine first.

19 MR. LEVINE: I wasn't proposing this as a
20 desirable situation, but I was proposing it as one that
21 was one that was not altogether implausible.

22 MR. HUSEMAN: Ryan Hamlin?

23 MR. HAMLIN: Yeah, and I think I was pretty
24 clear, I mean, from the get-go, we've said all along that
25 every group needs to have a seat at the table. We

1 certainly don't intend to exclude anybody. We are highly
2 incentive, because we are the ones that are opening our
3 checkbooks quite a bit today and spending millions and
4 millions of dollars, but certainly everyone will have a
5 seat at the table and a voice at the table. That was not
6 the intention at all.

7 MR. HUSEMAN: We have one more minute. I'm
8 going to bleed every last second out of you for this
9 forum, so one more question, and let's have it, Jennifer,
10 from the gentleman in the back there.

11 AUDIENCE MEMBER: I had a couple of questions,
12 actually. One is --

13 MR. HUSEMAN: Keep it very brief, please, you
14 have about 15 seconds.

15 AUDIENCE MEMBER: Okay, talk about the
16 combination of technology and legislation, but I wonder
17 if anyone could talk about the combination of technology
18 and economic incentives? There's Shred, there's
19 Vanquish, there's Bonded Sender. There's a lot of
20 proposals there. And then just regarding the do-not-e-
21 mail lists, I still would like to have someone explain to
22 me how there's not an easy directory, harvest attack on
23 such a do-not-e-mail list.

24 MR. HUSEMAN: Does anyone want to address the
25 directory harvest attacks?

1 MR. LEVINE: Talk to one of us later and we can
2 explain the technology. As far as e-postage, I have yet
3 to see an e-postage system that looks even faintly
4 implementable. So, at this point, it's just vapor-ware.
5 I don't think it's a practical approach.

6 MR. HUSEMAN: Okay. Steve Atkins, you have 15
7 seconds.

8 MR. ATKINS: Economic incentives, I-import,
9 bonded sender, looks viable, maybe-ish in some cases.

10 **(Laughter).**

11 MR. HUSEMAN: Great. Thank you. Now I'm going
12 to introduce Eileen Harrington, who will help conclude us
13 off.

14 **(Applause).**

15 MS. HARRINGTON: Isn't Brian wonderful?

16 **(Applause).**

17 MS. HARRINGTON: He's been working around the
18 clock on this for weeks, and here he is bleeding the last
19 second out of the forum. I can't believe it. I would
20 have been running out of the room by now, I think.

21 One of your colleagues said to me a minute ago,
22 it feels like this has been going on forever. I think
23 some of us wish that it could go on for a few more days,
24 because it's been so rich. And I think that we've saved
25 the best for the last, and with that I certainly don't

1 mean me, and I don't even mean my boss, Howard, who I'm
2 about to introduce, but this was really a wonderful panel
3 and very rich in information, in thought, in idea, in
4 challenge, and I want to thank all of you, and all of
5 you. This is sort of the end of Survivor, except there's
6 so many people left on the island.

7 **(Laughter).**

8 MS. HARRINGTON: I'm just amazed. I'd like to
9 introduce Howard Beales, who is my boss and our boss and
10 the Director of the Bureau of Consumer Protection at the
11 FTC. As Commissioner Swindle said this morning, at the
12 FTC, it's all about consumers. And Howard is the guy who
13 is responsible for carrying that flag. So, to wrap
14 things up for us, Howard Beales.

15 **(Applause).**

16 MR. BEALES: Thanks, Eileen. They always
17 schedule me at the end of these workshops, in case there
18 is nobody left.

19 **(Laughter).**

20 MR. BEALES: They figure commissioners might be
21 upset, but the bureau director, well, that's okay. I
22 want to -- we have come to the end of what I think has
23 been a very productive and a very exciting forum over the
24 last three or four days. I want to thank all of the
25 panelists who volunteered their time and expertise and

1 everybody in the audience who volunteered their time and
2 expertise to help educate us about the complexities and
3 the realities of the Spam problem.

4 I also want to thank Chairman Muris and the
5 commissioners who participated in the forum, Commissioner
6 Swindle, Commissioner Thompson, in particular, for
7 sharing their deep commitment to addressing and
8 responding to the many questions and concerns that are
9 out there about Spam.

10 And I want to thank the staff, who was really
11 tireless in putting together an outstanding workshop.

12 **(Applause).**

13 MR. BEALES: It's really easy to say, and I've
14 learned to say it very well, let's do a workshop.

15 **(Laughter).**

16 MR. BEALES: And it's very hard to actually do,
17 and they've done an outstanding job. Over the last three
18 days, we've heard from a number of people with different
19 perspectives on addressing the Spam problem. That
20 diversity of opinion has provided for a lively debate, a
21 very informative and I think a very informed discussion
22 on a great many issues.

23 The panel discussions I think have clearly
24 confirmed there isn't a simple magic solution, sad as
25 that may be, but they also illustrate that there are many

1 directions that we can take to try to protect e-mail for
2 consumers and for commerce. Many panelists discussed how
3 the swelling tide of Spam harms consumers and businesses
4 by imposing significant costs on them. Consumers find
5 themselves confronting unseemly images, spending time
6 deleting unwanted messages or not receiving valued e-mail
7 in lieu of receiving e-mails that promise immediate
8 wealth or a cure-all health care.

9 Businesses lose productivity because employees
10 spend time deleting unwanted e-mail. They spend more
11 money putting systems in place that will diminish the
12 amount of Spam that gets through their filters. Further,
13 there are costs, both large and small, that Spam imposes
14 on internet service providers.

15 Our panelists indicated that although the costs
16 are currently significant, they're going to give way to a
17 far greater harm, the loss of confidence in the powerful
18 communications medium of e-mail, and quite potentially
19 decreasing participation on the internet. We are at risk
20 of killing the killer-app.

21 The panelists also reaffirmed, there's a role
22 for continued aggressive law enforcement by the FTC and
23 other law enforcement authorities. We're certainly going
24 to continue to pursue vigorous enforcement against those
25 who threaten this communications medium, and the

1 marketing tool, by sending deceptive e-mail. We'll also
2 continue our efforts to educate consumers and businesses
3 in the steps they can take to decrease the amounts of
4 Spam and to recognize deceptive Spam when they see it.
5 We'll continue to study the issues; we'll continue to
6 take innovative steps to try to remain at the forefront
7 of stopping deceptive Spam and providing meaningful
8 consumer and business education. For example, you can
9 expect action from the FTC on the open relay issue in the
10 very near future.

11 One final housekeeping note, because of the
12 overwhelming interest in this conference, and because of
13 the turnout, I realize that many of you may not have had
14 the chance to make a comment or ask a question. We
15 invite you to supplement our record until May 16th. The
16 details and the instructions for doing so are on our web
17 page, at www.ftc.gov/bcp/workshops/Spam.

18 And speaking of this website, we're always
19 interested in sharing the information on it with
20 consumers and businesses. If you'd like to join us in
21 this effort, then please contact Charles Lawson in our
22 Office of Consumer and Business Education, at the risk of
23 having him overwhelmed, he's at clawson@ftc.gov.

24 Again, we feel strongly about the issues
25 concerning Spam, and I know that many of you are

1 passionate about these issues as well. I'm glad that
2 we've been able to host this thoughtful and productive
3 forum as a building block to address many of these
4 issues. My colleagues and I look forward to working with
5 you in the future. Thank you again for devoting your
6 time and effort to the forum, and thank you for staying
7 until the very end.

8 **(Applause).**

9 **(Whereupon, the hearing was concluded.)**

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 C E R T I F I C A T I O N O F R E P O R T E R

2 DOCKET/FILE NUMBER: P0244073 CASE TITLE: SPAM PROJECT4 HEARING DATE: May 2, 2003

5

6 I HEREBY CERTIFY that the transcript contained
7 herein is a full and accurate transcript of the notes
8 taken by me at the hearing on the above cause before the
9 FEDERAL TRADE COMMISSION to the best of my knowledge and
10 belief.

11

12

DATED: MAY 20, 2003

13

14

15

SONIA GONZALEZ

16

17

18

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

19

20 I HEREBY CERTIFY that I proofread the transcript for
21 accuracy in spelling, hyphenation, punctuation and
22 format.

23

24

25

SARA J. VANCE