

OFFICIAL TRANSCRIPT PROCEEDING**FEDERAL TRADE COMMISSION****MATTER NO. P024407****TITLE SPAM PROJECT****PLACE FEDERAL TRADE COMMISSION
600 PENNSYLVANIA AVENUE, N.W.
WASHINGTON, D.C. 20580****DATE APRIL 30, 2003****PAGES 1 THROUGH 309****FTC SPAM FORUM -- DAY ONE****SECOND VERSION**

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

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

Introduction to Spam	Page 2
E-mail Address Gathering	Page 78
Falsity in Sending of Spam	Page 173
Open Relays/Open Proxies/FromMail Scripts	Page 226

P R O C E E D I N G S

- - - - -

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

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

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

9 **(Group laughter.)**

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

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

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

1 if we have an evacuation.

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

6 **(Group laughter.)**

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

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

20 Mr. Chairman.

21 **(Applause.)**

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

25 Welcome to our forum on Spam E-mail and thank

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

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

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

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

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

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

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

11 During 2001, we received an average of 10,000
12 messages per day. Last year, that figure climbed to over
13 47,000. Currently we receive, into the refrigerator,
14 over 130,000 messages each day.

15 In February 2002, I announced the FTC's first
16 systematic crackdown on deceptive Spam. Since then, we
17 have tackled Spam on three fronts: Law enforcement,
18 education and research. To date, the FTC has announced
19 48 law enforcement actions targeting deceptive Spam.
20 Soon, we will announce a settlement in the first FTC law
21 enforcement action against false e-mail remove
22 representations and e-mail spoofing, by which Spammers
23 hide their identity through forging the from or reply
24 lines in e-mail messages.

25 In this case, the Commission has obtained its

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

3

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

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

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

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

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

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

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

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

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

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

1 adult and finance offers comprised 55 percent of our
2 sample.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

20 Welcome, Chairman Burns.

21 **(Applause.)**

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

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

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

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

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

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

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

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

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

20 **(Group laughter.)**

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

1 him for his dedication to this issue.

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

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

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

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

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

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

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

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

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

21 **(Group laughter.)**

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

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

12 Well, they must have hung there probably two or
13 three or four years, and I got a friend of mine, I got
14 this idea, because there was a couple of pairs of spurs
15 in there and they were pretty good. But they were old,
16 they had shown a little wear. And I just took a picture
17 of this pair and I advertised them as antique spurs from
18 Montana, put them on there. Them darn things brought
19 \$125 bucks.

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

21 **(Group laughter.)**

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

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

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

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

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

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

1 this morning.

2 **(Applause.)**

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

12 **(Applause.)**

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

18 **(Group laughter.)**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 forward to working with you in the days ahead.

2 Thank you.

3 **(Applause.)**

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

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

14 **(Applause.)**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 Thank you very much.

2 **(Applause.)**

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

8 Thank you very much.

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

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

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

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

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

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

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

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

14 MR. FERGUSON: Yeah.

15 MS. HARRINGTON: -- unsolicited?

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

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

25 MR. WIENZEN: Well, to me the issue here has

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

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

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

13 MR. WIENZEN: I expect nothing less.

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

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

1 difficulty has been mentioned.

2 We've met with the top people --

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

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

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

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

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

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

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

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

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

1 states.

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

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

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

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

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

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

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

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

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

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

1 changing and we're now into pop-ups.

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

7 **(Group laughter.)**

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

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

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

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

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

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

6 MR. COWLES: Correct.

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

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

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

22 MR. COWLES: Yes.

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

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

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

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

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

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

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

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

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

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

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

10 So, the reports that were talking about a 50
11 percent increase in Spam by the end of this year, were
12 wildly and naively over optimistic. We've seen more than
13 four-fold increase already this year, and it's going up
14 50 percent month-over-month at this point.

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

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

20 MS. HARRINGTON: Sure.

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

1 period of eight weeks. A huge amount of mail.

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

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

11 MS. HARRINGTON: Sure.

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

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

1 MR. FERGUSON: Can I respond?

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

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

9 MS. ATKINS: Yes.

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

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

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

20 MS. ATKINS: No.

21 MS. HARRINGTON: Okay.

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

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

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

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

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

20 MS. HARRINGTON: Okay. Laura?

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

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

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

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

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

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

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

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

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

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

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

18 MS. HARRINGTON: Okay. Thanks. Mark?

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

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

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

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

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

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

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

15 **(Group laughter.)**

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

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

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

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

5 Clifton?

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

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

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

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

17 Brian, where are you guys?

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

22 MS. HARRINGTON: What are the road blocks?

23 MR. ARBOGAST: My understanding is not strong
24 enough opportunity for ISPs and state agencies to enforce
25 --

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

22 **(Group applause. Bravo, bravo.)**

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

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

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

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

16 **(Group laughter.)**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8 **(Group boos.)**

9 **(Group laughter.)**

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

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

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

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

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

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

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

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

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

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

6 MS. HARRINGTON: Okay. Thank you. Mark?

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

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

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

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

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

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

1 MR. FERGUSON: It legalizes Spam.

2 MS. HARRINGTON: Okay.

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

13 MS. HARRINGTON: Okay. Thomas?

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

25 So, that would solve that problem, and it would

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

6 MS. HARRINGTON: You have a question, Laura?

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

12 MS. HARRINGTON: Speak in the mic, please.

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

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

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

20 **(Group laughter.)**

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

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

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

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

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

9 MR. COWLES: We do label everything.

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

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

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

25 MS. HARRINGTON: I have a quick question for

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

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

6 MS. HARRINGTON: And you block them?

7 MR. ARBOGAST: And we block it.

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

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

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

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

18 MS. HARRINGTON: Clifton?

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

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

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

10 MS. HARRINGTON: Okay. Bob?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

19 **(Group laughter.)**

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

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

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

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

10 **(Group laughter.)**

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

14 **(Applause.)**

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

17 MR. FRANCOIS: We have more time.

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

22 MR. FRANCOIS: No.

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

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

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

6 Your question? Identify yourself, please.

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

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

18 Chris, let me ask you your thoughts on that.

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

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

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

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

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

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

1 Next question? Where are my microphone people?

2 Okay, Jason? Make it quick.

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

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

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

10 MS. HARRINGTON: Joe?

11 MR. BARRETT: Opt-in.

12 MS. HARRINGTON: Clifton?

13 MR. ROYSTON: Definitely, opt-in.

14 MS. HARRINGTON: Chris?

15 MS. GREGOIRE: Opt-in.

16 MS. HARRINGTON: Laura?

17 MS. ATKINS: Opt-in.

18 MS. HARRINGTON: Brian?

19 MR. ARBOGAST: Opt-in.

20 MS. HARRINGTON: Bob?

21 MR. WIENTZEN: Opt-out.

22 **(Group laughter.)**

23 MS. HARRINGTON: Thomas?

24 MR. COWLES: Opt-out.

25 MS. HARRINGTON: Okay, okay. Next question?

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

4 INAUDIBLE NAME/QUESTION.

5 MS. HARRINGTON: Did I need to repeat that?

6 GROUP: Yes.

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

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

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

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

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

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

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

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

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

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

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

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

5 Mark says, no. Joe says --

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

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

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

12 MS. HARRINGTON: Chris?

13 MS. GREGOIRE: How do you enforce that?

14 MS. HARRINGTON: Okay. Laura?

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

17 MS. HARRINGTON: Okay.

18 MR. ARBOGAST: It's a bad idea.

19 MS. HARRINGTON: Bob?

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

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

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

4 MS. HARRINGTON: Yes.

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

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

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

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

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

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

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

1 past six to seven years.

2 MS. HARRINGTON: The room is electric.

3 **(Group laughter.)**

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

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

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

14 EMILY: There's a class action suit --

15 MS. HARRINGTON: Class action suit in Utah.

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

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

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

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

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

14 MARIE GEORGES: In a fair way.

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

22 MR. ARBOGAST: Can I answer that question?

23 MS. HARRINGTON: Yes, Brian.

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

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

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

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

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

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

20 We have a question over here.

21 **(Inaudible speaker identification/question.)**

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

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

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

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

12 Mark?

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

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

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

25 MS. HARRINGTON: All right. None of this,

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

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

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

11 **(Applause.)**

12 **(Whereupon, there was a 15-minute break from**
13 **10:15 a.m. until 10:30 a.m.)**

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

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

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

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

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

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

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

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

25 Then we have Doug McLean, who's the Vice

1 President for Corporate Marketing for Postini,
2 Incorporated.

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

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

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

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

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

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

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

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

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

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

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

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

13 **(Group laughter.)**

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

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

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

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

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

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

10 Depending on the site you're hitting, how fast
11 your connection is -- I think during a test last night I
12 was collecting about 200 mails every two minutes -- about
13 100 mails a minute for this particular tool. So, you can
14 get a pretty good collection of lists.

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

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

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

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

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

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

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

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

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

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

22 **(Group laughter.)**

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

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

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

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

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

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

18 MR. WENGER: And how does this verification
19 work?

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

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

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

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

11 MR. STEELE: Yeah.

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

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

25 MR. WENGER: Like a handshake between two

1 people.

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

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

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

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

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

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

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

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

9 **(Group laughter.)**

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

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

25 The other thing that's not really shown here,

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

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

10 MR. WENGER: Okay, great. Thank you.

11 MR. STEELE: Thanks.

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

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

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

20 MR. desJARDINS: (Complies.)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

10 **(Group laughter.)**

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

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

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

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

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

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

25 Just to deal with the part of our study that

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

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

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

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

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

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

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

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

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

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

25 MR. WENGER: But your intention is that if you

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

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

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

21 **(Group laughter.)**

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

1 MR. COURTNEY: Exactly.

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

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

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

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

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

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

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

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

16 **(Group laughter.)**

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

1 Thanks very much.

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

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

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

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

25 To give you an idea, I would recommend for

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

19 Thank you.

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

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

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

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

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

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

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

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

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

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

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

1 actual deliveries on the AOL system, and guess what?

2 It's also about 75 percent junk.

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

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

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

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

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

14 So, what eventually happens is, they hit a good
15 one; they immediately open an SMTP session and send a
16 piece of Spam. Or, they may just wait until it collected
17 15 or 20,000 addresses and do that all at once a little
18 bit later.

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

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

1 these directory harvest attacks. It only takes us about
2 12 invalid calls to identify that and block it. We have
3 a number of technical techniques for doing that and
4 during the Q&A maybe we can dive into that.

5 We map these things every single day on our
6 website. I'm afraid this map probably doesn't resolve
7 very well for a lot of you, but the red and the purple
8 dots that you see on this map are the directory harvest
9 attack sources that we saw one day back in January.

10 There were only 40 millions messages that day for us, it
11 wasn't a huge day, but we saw 20 million pieces of Spam.

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

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

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

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

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

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

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

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

7 And that's me, thank you.

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

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

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

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

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

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

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

17 MR. WAGGONER: I want to add something.

18 MR. WENGER: Okay, go ahead, sure.

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

24 MR. STEELE: Yeah.

25 MR. WAGGONER: And dictionary attacks, I mean,

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

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

10 MR. STEELE: Yeah, we do.

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

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

23 MR. WAGGONER: Thanks.

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

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

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

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

25 MR. WENGER: An interesting point has been

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 of websites all over the internet --

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

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

8 MR. WENGER: Okay.

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

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

14 MR. WAGGONER: Typically, no.

15 MR. WENGER: No.

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

1 we develop our list, generally over the --

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

4 MR. WAGGONER: Yes, exactly.

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

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

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

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

22 MR. WENGER: The world?

23 MR. WAGGONER: Yeah.

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

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

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

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

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

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

1 mortgage leads or whatever the product might be.

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

7 MR. WENGER: Okay.

8 MR. WAGGONER: Does that make sense?

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

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

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

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

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

17 MR. WENGER: Like Gogle --

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

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

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

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

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

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

14 MR. desJARDINS: No.

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

17 MR. desJARDINS: That's correct.

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

25 I mean, if you can show me a website that

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

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

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

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

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

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

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

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

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

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

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

1 just -- it's garbage.

2 MR. WENGER: Two billion they said.

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

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

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

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

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

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

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

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

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

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

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

22 MR. WENGER: Netiquette kind of rules, right.

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

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

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

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

25 MR. STEELE: Yeah, I do work for Brightmail

1 actually.

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

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

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

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

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

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

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

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

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

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

25 MR. WAGGONER: Oh.

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

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

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

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

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

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

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

25 **(Laughter).**

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

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

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

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

25 MR. WENGER: Not in this room.

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

5 MR. WENGER: Does that work?

6 **(Laughter).**

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

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

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

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

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

21 MR. TERRIBERRY: Mm-hmm.

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

25 MR. TERRIBERRY: They're a vendor.

1 MR. WENGER: Okay, so they --

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

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

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

8 MR. WENGER: Mm-hmm.

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

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

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

23 MR. WENGER: Right.

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

1 do is reply to the e-mail.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7 MR. WENGER: Right.

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

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

14 MR. TERRIBERRY: Absolutely.

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

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

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

8 MR. WENGER: But is that because --

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

12 MR. WENGER: -- they're not opening messages or
13 because they're not -- right. Or is it because the
14 messages are not getting through? Is it a combination of
15 --

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

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

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

25 MR. WENGER: Right.

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

4 MR. WENGER: Right.

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

9 MR. WENGER: Right.

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

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

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

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

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

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

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

10 Richard, did you have something?

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

13 MR. WENGER: Okay.

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

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

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

12 MR. WENGER: The question is how much?

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

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

16 MR. WAGGONER: Thousands, there we go.

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

19 MR. TERRIBERRY: Yeah, back to --

20 **(Laughter).**

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

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

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

6 MR. WENGER: Right.

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

9 MR. WENGER: Right.

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

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

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

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

24 UNIDENTIFIED SPEAKER: Which may be embedded in
25 the newsletters.

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

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

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

25 MR. WENGER: The question that preceded that,

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

4 Yes, over next to Stephen here.

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

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

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

1 MR. TERRIBERRY: Actually, the technology --

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

22 MR. WENGER: Jeff Fox from Consumers Union?

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

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

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

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

25 Right, and he gave an example of having filed a

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

6 Mona, you have an e-mail?

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

9 MS. SPIVACK: Yeah.

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

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

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

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

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

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

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

14 MR. COURTNEY: Right.

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

18 MR. COURTNEY: Right.

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

25 MR. COURTNEY: That's right.

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

7 MR. TERRIBERRY: Too many to list.

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

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

11 MR. WAGGONER: Right.

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

14 MR. WAGGONER: Right.

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

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

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

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

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

9 MR. WAGGONER: We never --

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

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

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

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

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

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

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

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

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

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

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

1 MR. TERRIBERRY: No.

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

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

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

21 MR. TERRIBERRY: If they do --

22 MR. WENGER: Look at the advertisement.

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

24 -

25 MR. WENGER: Right.

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

6 MR. WENGER: Right.

7 MR. TERRIBERRY: That maintains the value.

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

10 MR. TERRIBERRY: Right.

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

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

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

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

23 MR. WENGER: Maybe we could have him step up to
24 this microphone here actually, because he's so close to
25 it anyway, and then I wouldn't have to repeat what he

1 says.

2 MR. LEWIS: Okay, how's that?

3 MR. WENGER: The one to your left there.

4 MR. LEWIS: The other one, okay.

5 **(Laughter).**

6 MR. LEWIS: My name's Chris Lewis, I'm with
7 Nortel Networks, I'm going to be on a panel tomorrow.
8 I've got a couple of numbers that will be of direct
9 relevance to what was just talked about today, but I'm
10 not going to be talking about my economics session
11 tomorrow. And that is there was a comment today or just
12 recently about how it appears that harvested e-mail
13 addresses disappear quickly from spam.

14 And our experience is the exact opposite. As a
15 very good example, we had a series of domains that we de-
16 registered, or actually we de-MXed, technically. It
17 means we made it unreachable. You could not send mail to
18 this anymore. At the time we turned it off, two and a
19 half years ago, it was receiving between 60,000 and
20 70,000 pieces of spam a day. Out of curiosity, I turned
21 it back on again two months ago, and it was at 600,000
22 per day.

23 These are addresses that were completely and
24 totally undeliverable for over a year. And it went from
25 50,000 to 600,000.

1 MR. SMITH: Can I make one comment here?

2 MR. WENGER: If you speak into the microphone.

3 MR. SMITH: I think that what the CDT study
4 showed is that if those -- any addresses still appear on
5 websites then they'll still get spam.

6 MR. LEWIS: Oh, these have been
7 administratively terminated through everything, because
8 that is our corporate face, is those domain names. The
9 other comment I wanted to make was -- is to stress the
10 issue of dictionary attacks. I mean, people were talking
11 about that today and they were talking about hundreds of
12 thousands. I just wanted to mention that we have a
13 series of undoing 6 to 7 million per day, and we're
14 blocking entire countries because of this. This is how
15 bad it's getting. Thanks.

16 MR. WENGER: Okay, I'd love to take more
17 questions. I see more hands out there, but I'm being
18 told that we're done here. So, I have -- I'm going to
19 turn the microphone over to Renard Francois for a brief
20 announcement, and then we'll see you back here at 1:30.

21 MR. FRANCOIS: Before you all leave, we have
22 several important announcements to make, and I will try
23 and do them as quickly as possible. First, name tags, if
24 you are a panelist or an audience member, you should hang
25 onto your name tags; panelists for the duration of the

1 forum; audience members for the day. So, if you go out
2 to lunch, please bring your name tags, otherwise you will
3 have to sign up and get new ones. But whether you are
4 panelists or audience members, you will still have to go
5 through security if you exit the building, okay?

6 Second, capacity. It's still first-come,
7 first-serve with the chairs. And once we hit capacity,
8 we will be turning people away and directing them to the
9 overflow rooms, which I'm told has copious amounts of
10 space. There are about 20 people in each overflow room,
11 and we've corrected the problems that 432 is experiencing
12 with audio. Even if your belongings are in here and
13 we've reached capacity, there is -- we still won't be
14 able to accommodate you.

15 MR. WENGER: So people should take their
16 belongings?

17 MR. FRANCOIS: Yes. Camera lights. We know
18 for people over here we've received some complaints about
19 the camera lights, those are C-Span lights. We're told
20 that if they remove them they will not be able to get the
21 audience, so we apologize for the inconvenience, but
22 they're going to be there.

23 This is for the media. Interviews cannot be
24 done in the galley, which is the hallway behind the
25 center; cannot be done in the conference lobby and cannot

1 be done in the building lobby. They can be done in the
2 green room and outside of the building, as long as it
3 doesn't obstruct the entranceway. If you have any
4 questions, you can see Brian, Sheryl or myself or Mona or
5 Voni.

6 MR. WENGER: Anybody with a green.

7 MR. FRANCOIS: Right. The other thing is
8 temperature. We've heard other complaints about
9 temperatures. As an addition, if you think this is cold,
10 you should come to a commission hearing.

11 **(Laughter).**

12 MR. FRANCOIS: But we've been told that it will
13 neither go up nor down, so for tomorrow, pack a sweater.

14 Page 2 of the bios, some people didn't receive
15 page 2. Those are outside on the registration table.
16 And the last thing is we will have Senator Charles
17 Schumer coming in at about -- at approximately 1:30 to
18 deliver some comments. The next panel will start shortly
19 thereafter, it's Falsity in Spam.

20 Thank you.

21 MR. WENGER: Okay, thanks, everybody, for
22 coming, and we're going to be starting sharply at 1:30,
23 so please be back in your seats at that point. Thank
24 you.

25 **(Whereupon, a lunch recess was taken.)**

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

AFTERNOON SESSION

- - - - -

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

1 MS. HARRINGTON: Good afternoon. We're back.
2 A couple of announcements quickly before we turn to
3 Senator Schumer. If you've got your cell phone on, turn
4 it off, or we'll send you wireless SPAM. Remember that
5 in the unlikely event of an evacuation, just go out the
6 door. And that covers the security stuff. You also have
7 to keep your badge on for the duration, or you'll go
8 through sort of security purgatory to get in.

9 We are so lucky to have Senator Schumer with us
10 this afternoon. He has worked closely with the Federal
11 Trade Commission in his capacity as a member of the
12 Senate Judiciary Committee. And most recently we were
13 delighted to have him involved in the discussion of the
14 Commission's generic drug study. He has long been a
15 tireless advocate for consumers. And as many of you
16 know, he has recently been discussing possible
17 legislative solutions to the burden that consumers are
18 confronting in their e-mail boxes.

19 And, so, without any further ado, the Senior
20 Senator from the State of New York, the Honorable Charles
21 Schumer. Thank you.

22 **(Applause).**

23 SENATOR SCHUMER: Thank you, Eileen. Well,
24 thank you. It's good to be here with everybody, and
25 first, before I get into the substance of my remarks, I

1 do want to tell you that I hope my speech today goes a
2 little better than one I gave back in my old former
3 Congressional District, the 9th CD in Brooklyn, because
4 at the end of my speech, one of the senior citizen
5 activists who populate the 9th CD in big numbers came
6 over to me and she said, Senator, I thought your speech
7 was absolutely superfluous.

8 **(Laughter).**

9 SENATOR SCHUMER: Well, I didn't want to let
10 that remark go unanswered, so I responded. I said, Thank
11 you very much, ma'am, I plan to publish it posthumously.

12 **(Laughter).**

13 SENATOR SCHUMER: But the senior citizen
14 activists always get the last word in in the old 9th CD.
15 She put her hands on her rotund hips, she waved her
16 finger in the air and said, Senator, I just can't wait.

17 **(Laughter).**

18 SENATOR SCHUMER: So, I hope today what I have
19 to say is not superfluous. I doubt it will be published
20 posthumously or otherwise, but I'm very glad to be here
21 to give you some brief remarks.

22 And first I would say to all of you that we are
23 under siege. Armies of on-line marketers have over-run
24 e-mail inboxes across the country with advertisements for
25 herbal remedies and get-rich-quick schemes and

1 pornography. The Spam forum taking place here over the
2 next three days comes not a moment too soon as we decide
3 how to organize our counter-attack.

4 And I want to commend the FTC and Eileen
5 Harrington, in particular, wherever she went, there you
6 are, for bringing us here today. It is my hope that the
7 impressive roster of panelists and speakers that you'll
8 listen to and discuss issues with will stimulate ideas on
9 how to stop the Spammers in their tracks. I have a
10 number of thoughts of my own over the next few weeks and
11 months that I'll be pursuing in Congress.

12 Now, as you are all aware, Spam traffic is
13 growing at a geometric rate, causing the super-highway to
14 enter a state of virtual gridlock. What was a simple
15 annoyance last year has become a major concern this year,
16 and could cripple one of the greatest inventions of the
17 20th Century next year, literally next year, if nothing
18 is done.

19 Way back in 1999, the average e-mail user
20 received just 40 pieces of unsolicited commercial e-mail,
21 what we call SPAM, each year. This year, the number is
22 expected to pass 2,500. I know I'm lucky if I don't get
23 40 pieces of SPAM every couple of days. As a result, a
24 revolution against SPAM is brewing as the epidemic of
25 junk e-mail exacts an ever-increasing toll on families,

1 businesses and the economy.

2 And let me illustrate this point with a
3 personal story. My wife and I have two wonderful
4 children, one of whom is about to complete her first year
5 at college. The other, age 14, she's an absolute whiz on
6 the internet. She loves sending and receiving e-mail.
7 She spends far more time at the computer than she does
8 watching television, which, in general, is a great
9 advance.

10 As parents, we do our best to make sure she has
11 good values and that the internet is a positive
12 experience for her, a device to help her with her
13 schoolwork or learn about events taking place around the
14 world and maybe even a way to order the latest 'N Sync
15 CD. But you can imagine my anger and dismay when I
16 discovered that not only was she a victim of SPAM like
17 myself, but like all e-mail users, much of the junk mail
18 she was receiving advertised pornographic websites. I
19 was and remain powerless to prevent such garbage from
20 reaching my daughter's inbox.

21 The frustration I feel in the battle against
22 Spam is one that I think business owners and ISPs across
23 the nation can identify with. According to Ferris
24 Research, Spam cost businesses in the United States \$10
25 billion each year in lost productivity, consumption of

1 information technology resources and help desk time.
2 With surveys showing that over 40 percent of e-mail
3 traffic qualifies as Spam, we all know that ISPs spend
4 millions of dollars each year on research, filtering
5 software and new servers to deal with the ever-expanding
6 volume of junk e-mail being sent through their pipes.
7 They're doing a good job, but you know in this battle of
8 offensive and defensive warfare, I'm afraid the Spammers
9 always get a leg ahead and figure out a way around the
10 filter. And that's why it's time for the Federal
11 Government to step in.

12 And I was utterly amazed to learn, when I
13 started looking into this, that Spamming is not a crime,
14 unless you commit fraud, like everywhere else. And, so,
15 over the next couple of weeks, I'll be unveiling a series
16 of bills to clamp down on junk e-mail. And the
17 legislation we will introduce will have two new weapons
18 in the battle against Spam.

19 First, a Federal no-Spam registry modeled on
20 the FTC's recently introduced do-not-call list. And
21 second, for the first time, tough criminal penalties for
22 repeat violators of new Spam regulations. Maintained by
23 the FTC, the no-Spam registry will be a gigantic data
24 base of people who have opted out of receiving Spam by
25 submitting their e-mail addresses to the list. The model

1 for this innovation are the do-not-call registries that
2 have been used to ward off telemarketers.

3 The FTC has just inaugurated its national no-
4 call registry and expects telemarketing calls to decrease
5 80 percent as a result. We've had one in my State of New
6 York. We signed up early on, and instead of at dinner
7 jumping up, you know, like jack rabbits every three
8 minutes to answer the phone, it has not ended these kind
9 of calls, but it's curtailed them.

10 Now, critics have raised doubt about the
11 registry, arguing it violates free speech or that it
12 really doesn't prevent Spammers from sending e-mails, and
13 it creates the very thing Spammers cherish most, a
14 precious list of millions of e-mail addresses to which
15 they can peddle their wares. Let me be clear, under my
16 plan, Spam will refer exclusively to unsolicited
17 commercial communication. That is a category of speech
18 that doesn't qualify for full First Amendment protection,
19 and it's been successfully regulated numerous times over.

20 And any Spammer that sends e-mail to addresses
21 in the registry will be committing a crime punishable by
22 stiff fines and potential jail time down the road. They
23 don't get jail time; you first get a warning; you keep
24 doing it in large magnitude, fines of up to \$5,000 per
25 day; and you keep doing it after that, it's jail time up

1 to two years. Now, these are the same devices we use to
2 prevent more traditional crimes.

3 Meanwhile, the data base will be protected by
4 military-caliber encryption, so that its valuable
5 contents won't fall into the wrong hands. The list will
6 be salted with dummy addresses, so that in the unlikely
7 event that a Spammer cracks its protective codes and uses
8 its content, FTC officials will be able to track down the
9 offender and subject the Spammer to criminal prosecution
10 for felony theft of Federal property.

11 Is it easier to go after the telemarketers than
12 the Spammers? Yes. But there's one fact that underlines
13 our enforcement effort, and I think that is key, and
14 that's true with everything in terms of enforcement, and
15 that is that 90 percent of Spam, 90 percent, is just sent
16 by 150 spammers. So, that it's a small number who are
17 doing most -- creating most of the problem. And as
18 you'll see, we give the FTC the resources to go after
19 those people, and that's how we can succeed here. We
20 won't stop all of it, but this registry will stop a whole
21 lot of it, particularly the big guys who do most of the
22 damage.

23 Now, we also give the right for the FTC, state
24 attorneys and ISPs to seek civil penalties against
25 Spammers for the amounts of damages, I said, up to \$5,000

1 per offense. But of equal importance, the FTC is going
2 to have the funds needed to carry out this new mission.
3 The no-spam registry and tough enforcement measures will
4 not become unfunded mandates.

5 Originally, someone proposed that we put \$75
6 million in this, which Congress would gladly allocate to
7 get rid of spam, but we heard that's more than 50 percent
8 of the whole FTC budget already, so it will probably be
9 less than that, but money, Eileen, money will be no
10 object.

11 **(Laughter).**

12 SENATOR SCHUMER: You'll be able to do whatever
13 you need. Now, my plan doesn't stop there, although
14 that's the heart of it.

15 MS. HARRINGTON: That's the most important part
16 of it.

17 **(Laughter).**

18 SENATOR SCHUMER: That's right. And, by the
19 way, again, free speech objection, not to a telemarketing
20 registry, because you have the right to say you don't
21 want to hear, see, get something in the mail. That's
22 completely consistent with the First Amendment and of
23 course we're dealing with commercial speech anyway.

24 But here are some other things we do. In
25 addition to the two central provisions of criminal

1 penalty and the registry, we're going to take aim at mass
2 collection of e-mail addresses and the rampant fraud,
3 which, according to a report released by the FTC, is
4 present in 66 percent of junk mail. My legislation will
5 ban the hated practice of e-mail address harvesting,
6 affording internet service, chat room participants and
7 news group users a new level of protection from Spambots.

8 Subject headings, headers, domain names and
9 router information of commercial e-mail will have to
10 accurately reflect the content and source of the
11 messages. All commercial e-mail will have the letters
12 ADV, capital ADV, in the subject line, indicating that it
13 contains a message with commercial content. The ADV
14 heading, of course, is particularly useful because it
15 will allow filters to easily separate the spam from the
16 personal or business-related e-mail users receive each
17 day. And any commercial e-mail without a valid
18 unsubscribed address will be considered illegal.

19 The skeptic, of course, will say that all of
20 these are great ideas but hard to implement in practice,
21 especially given that the internet makes sending spam
22 incredibly inexpensive and easily anonymous. That's why
23 at the heart of this legislation are the tough penalties
24 and the enforcement dollars. Yes, it will take a while
25 to chase these folks down, but again, because 90 percent

1 is sent by 150 Spammers, you go after the big ones, keep
2 them on the run and we'll make a real dent here. We will
3 really make a dramatic, dramatic difference.

4 So, as you can see, this is a comprehensive
5 plan. It addresses the technical problems associated
6 with stopping Spam in its tracks; provides effective
7 enforcement mechanisms to end this insidious fraud and
8 harassment by peddlers of pornography, financial scams
9 and deceptive advertising. And I fully expect it to turn
10 the tide in our battle against spam.

11 I should add if you're a legitimate company,
12 you'll have nothing to fear from this legislation.
13 Indeed, I believe you should get on board as one of its
14 chief advocates, because right now people are so
15 frustrated at the junk e-mail bombardment that they
16 delete everything, including legitimate commercial e-
17 mail, as if it were spam. Implementing these rules means
18 it's more likely your message will be read.

19 I hope this plan provides you all with fruitful
20 fodder during your discussion over the next couple of
21 days. I am interested in your feedback. If any of you
22 have other ideas, ways to improve what we're doing, we're
23 just at the beginning here, I'm a member of Judiciary
24 Committee. It's Judiciary and Commerce that have joint
25 jurisdiction over this. We welcome them, and please

1 don't be shy. You will be able to send us an idea by e-
2 mail, by calling us, by whatever, and we will try to
3 incorporate them. So, contact my office if you have
4 other ideas.

5 I'm excited about the upcoming legislation, and
6 knowing the wide public distaste for spam, I believe that
7 support from other members of Capitol Hill will be
8 forthcoming. I'd be very, very surprised if we didn't
9 pass a comprehensive anti-Spamming bill this session of
10 Congress.

11 Thank you very much.

12 **(Applause).**

13 MR. COHEN: Thank you. Well, Senator Schumer
14 will be a hard act to follow, but we'll try. Welcome to
15 the Falsity in Sending of Spam panel. My name is Stephen
16 Cohen. I am a Staff Attorney in the Division of
17 Marketing Practices at the Federal Trade Commission.

18 With me on the panel today is Margot Koschier,
19 who is the Manager of the Anti-Spam Analysis and
20 Prevention Team at AOL. Chris Jay Hoofnagle is the
21 Deputy Counsel of the Electronic Privacy Information
22 Center. Bryan Bell is the Senior Abuse Investigator at
23 MCI. William Plante is Director of Worldwide Security &
24 Brand Protection at Symantec. Samuel Simon is Chairman
25 of the Telecommunications Research & Action Center. And

1 Scott Richter is President of Optinrealbig.com.

2 We're going to start out this session with
3 Margot doing a presentation on falsifying header
4 information and spoofing.

5 MS. KOSCHIER: Okay, everybody, thank you for
6 the introduction. I have been asked to do a brief
7 technical introduction into what the technical
8 specifications of e-mail falsification are. And in order
9 for you to adequately understand those, you need to know
10 what is good -- what are good headers from what are bad
11 headers. You need to be able to draw that distinction.
12 So, we'll do basically an intro to e-mail, what TCP/IP,
13 DNS and SMTP are, and then I will do a forgery of an e-
14 mail.

15 Okay, TCP/IP is transmission control
16 protocol/internet protocol. It's the language used by
17 machines, of which the internet is composed. Each
18 machine is connected to each other to communicate with
19 one another. IP is responsible for moving packets of
20 data between the servers and nodes; and TCP is
21 responsible for verifying data delivery from client to
22 server. Client is a term that refers to a freestanding
23 machine that acts on another machine. The server is the
24 one that serves it with data.

25 If you have more questions -- this is like

1 30,000-foot level here, in this dog-and-pony show, so if
2 you have more questions, I refer you to [www.rfc-](http://www.rfc-editor.org)
3 [editor.org](http://www.rfc-editor.org). RFC 791 and 793 will go into more detail on
4 that. And at the bottom of each one of these slides, if
5 there are relevant RFCs, I put the basic ones on there,
6 so for your knowledge.

7 Okay, IP addresses are coordinates used to
8 locate where servers on the internet are with respect to
9 each other. Every machine connected to the internet has
10 an IP address, and I apologize if this is like common
11 knowledge, but I just want to bring everybody to the same
12 base level here. The format of an IP address is a 32-bit
13 numeric address written as four numbers separated by
14 periods, for example, 208.15.23.1. Each set of numbers
15 is termed an octet or net block, and each octet can be 0
16 to 255, so 256 characters potentially. RFC 791 has more
17 information on that.

18 DNS. Domain name system is a distributed
19 internet directory which associates a domain name, like
20 aol.com or ftc.gov, and the IP addresses of the servers
21 which belong to that domain name. Most internet services
22 rely on DNS to work, and if DNS fails, websites can't be
23 located and e-mail delivery stalls. Good tools to help
24 you determine which IP addresses are associated with
25 which domain names and vice versa are NS Lookup and Trace

1 Route from a networked Unix host.

2 And if you don't have that kind of access to
3 your mail servers, your systems administrators are a
4 little more protective and I encourage you to go to
5 www.samspace.org or mayeast, which is a really long URL.
6 I think my thingy here, my slide show's up on the
7 website, so if you need it, you can get it from there.
8 Trace Route and NS Lookup are on those websites.

9 SMTP, simple mail transfer protocol, is the
10 procedure which generally happens on port 25, by which e-
11 mail data packets are transferred from one machine to
12 another. They are thousands of different types of
13 software which speak SMTP. Some software packages are
14 free; others are not. SendMail is the most widely used,
15 available software. It's virtually free and pretty darn
16 reliable. And then I list some other software products.
17 RFCs 821 and 822 talk about the creation and formulation
18 of an SMTP transaction.

19 Okay, here's an SMTP example. Matthew from
20 Brightmail came up and did a presentation a bit ago on
21 his harvesting tool and you saw little pieces of an SMTP
22 transaction in there. Here's another one. Basically I
23 said Telnet, which is on port 23, to Yahoo's mail server
24 on port 25. I connected to it. Over here, I said, Hi,
25 I'm from aol.com, because I was. He said, Okay, this is

1 my name. I said, I want to send mail from
2 mkosch@aol.net, which is one of my e-mail addresses, to
3 testforftc@yahoo.com, which is an e-mail address I
4 created for illustrative purposes today.

5 They said, Okay, the recipient,
6 testforftc@yahoo.com exists. I said, Okay, now I'm going
7 to send my data. He responded, 345, okay, go ahead. And
8 then I typed in the date, April 28th, which was the time
9 of the test from me; the subject; and then I ended the
10 transaction with a period on a line by itself, and it
11 said, 250, okay, I don't know what dirdel is, if somebody
12 wants to tell me, I'd be -- Miles Linear in the audience?

13 Okay, cool, delivery. And then I quit out; and
14 he said okay, bye-bye. So, if we take a look at that
15 actual header on the mail, here's my test mailbox. Wow,
16 this is pretty slow. You guys ever think about AOL
17 Broadband?

18 **(Laughter).**

19 MS. KOSCHIER: Okay, this is not the full
20 message, but let's take a look at the full headers here.
21 And come on, little guy. Here we go. Headers, as I will
22 talk about in a second, are stamped in the order in which
23 the packet is received to machine. So, the bottom-most
24 header line, which is this received from, is technically
25 where it originated. So, I was actually signed on to

1 that IP address. That was my helo string. Remember, I
2 typed helo, aol.com. And then I connected to Yahoo mail
3 server, and then the mail connected to Yahoo and was
4 delivered to the mailbox.

5 My from address, I said I was mkosch@aol.net,
6 Margot, and the X apparently to -- who it was to was
7 testforftc. Pretty straightforward.

8 Okay. Headers are the mess of received from
9 lines, I just showed at the top, or bottom, of an e-mail
10 message, depending on which client you're looking at.
11 They are a recorded log of the specific route a
12 particular e-mail took from its destination to its
13 arrival point. Theoretically, they're stamped by every
14 machine an e-mail packet hits in order from bottom to
15 top. As we will find out in the next panel on proxies
16 and open relays, sometimes headers aren't stamped. There
17 are tricky things that you can do to outwit machines.

18 So, theoretically, the topmost received line in
19 the header is the last machine an e-mail touched before
20 it arrived in your mailbox. One thing to remember is
21 since you don't have any pre-existing knowledge about
22 where an e-mail went before it got to your system, the
23 only header information that is reliable is the IP
24 address that is connecting to your mail server to send
25 that mail. Everything else could be totally faked and

1 forged.

2 And, let me just show you those headers.

3 Here's how easy it is to forge an e-mail. What I'm doing
4 now, if I'm still connected to my internal network, I
5 might have been booted. Yep, okay, I'm not -- obviously
6 having typing problems. I'm doing an NS Lookup like I
7 specified before. I'm saying I want the mail servers for
8 yahoo.com. Here are their mail servers, right here. So
9 I'm going to telnet to one of them, on port 25. I'm
10 connected. Helo, senate. Oops, sendate.gov, okay,
11 sorry. Let's see, e-mail from -- who would be a good
12 person to forge? Timothy Muris.

13 **(Laughter).**

14 MS. KOSCHIER: At ftc.gov. Resp 2, test for --
15 uh-huh, typo, okay. They're not open relays, everybody,
16 take a look at that, relaying denied. No surprise from
17 Yahoo. Test for FTC -- chalk it up to nervousness. All
18 right. Cool. Here's where I say data. I'll do the
19 date. Let's say it's August 13, 2024. From
20 tmuris@ftc.gov. Subject, anyone know where I can buy
21 some spurs?

22 **(Laughter).**

23 MS. KOSCHIER: Yeah, this is a test. All
24 righty. This user doesn't have a Yahoo account.
25 Testforftc@yahoo.com. That's surprising. I could have

1 sworn I have a Yahoo account. Test for -- did I spell it
2 wrong? Oh, okay. Do that again, I'm sorry, gang.

3 Indeed I could have. Helo, ftc.gov, mail from,
4 okay, data, date, Margot. Cool, we're done. Let's get
5 out of there. All right, so it wasn't as easy as I
6 thought it was going to be, but as soon as Yahoo decides
7 to deliver the mail, we'll see that in my inbox. I have
8 e-mail from -- good presentation from Yahoo.com. All
9 right, who's the punk in the audience?

10 **(Laughter).**

11 MS. KOSCHIER: All righty. A good
12 presentation. That's really funny, gang. Ha, ha, ha.
13 Okay, if we take a look at the other one, on to more
14 serious things, we've got a mail from some kluged e-mail
15 address, still looking for spurs. And if we take a look
16 at the headers of it, it's from tmuris@ftc.gov. You can
17 still see the connecting IP address, like I indicated
18 before, that's really the only reliable information of
19 where this transaction is coming from.

20 I just happen to be logged in to our internal
21 network at AOL to send this message, because that's the
22 only way I can get to a Unix prompt, but it's extremely
23 easy to forge header information. I really encourage you
24 to take a close look at headers, see if the FTC -- take a
25 look at samspade.org, see if the FTC has any kind of

1 authoritative answer with 152.163, and you're going to
2 see that it's not, it's AOL, obviously there's something
3 fishy there. So, that's pretty much what I have.

4 MR. COHEN: Thank you, Margot. And thank you
5 to the Yahoo guys.

6 **(Applause).**

7 MR. COHEN: So, my first question is to all of
8 our panelists, after seeing this, is why was e-mail
9 designed to make it so easy to forge identities. Anyone
10 who wants to answer that?

11 MR. BELL: Well, I will. It was back when the
12 protocol was designed, security, forging and what they're
13 going to do with e-mail nowadays was not thought into the
14 protocol.

15 MR. COHEN: Any other thoughts? Sam?

16 MR. SIMON: Just a point, there was an ethic a
17 long time ago that commercial -- I mean, it was designed
18 when commercial e-mail wasn't even part of the internet.
19 The whole idea of the internet was to be for the sharing
20 of ideas among people and colleagues. And what the
21 internet has become is certainly not even close. You
22 know, you could use a variety of adjectives, compared to
23 what it was originally intended to be.

24 MR. COHEN: This is a question for Bryan,
25 Margot and Scott. What portion of the e-mail industry

1 uses falsity in their spam, such as false subject lines
2 and false removal representations?

3 MR. BELL: Well, about 60 percent of the
4 complaints that we get at MCI have either false headers,
5 false e-mail addresses or deceptive subject lines, or a
6 combination of all three.

7 MR. COHEN: Scott, do you have anything?

8 MR. RICHTER: No, I wouldn't have any comment
9 on that. I don't do that, so I really can't answer.

10 MR. COHEN: Well, but in your experience with
11 other bulk e-mailers, do you have any idea?

12 MR. RICHTER: No, I've never seen any
13 statistics on that.

14 MR. COHEN: What percentage of spam -- this is
15 also for the same group -- of spam have falsified routing
16 information?

17 MR. BELL: I'd go back to my previous
18 statement. It's hard, you know, about 60 percent have
19 one of the three in the actual e-mail headers, falsifying
20 information.

21 MR. PLANTE: If I could just add one comment.

22 MR. COHEN: Sure.

23 MR. PLANTE: Speaking to the Symantec
24 experience, it used to be maybe six months to 12 months
25 ago when we began investigating spams that involved a

1 Symantec product that it was relatively easy to trace who
2 was sending it and in some way or other interdicted,
3 especially if it were, in our particular case, a
4 counterfeited material.

5 In the last several months, the spammers that
6 are using this type of technique are becoming more and
7 more sophisticated in their ability to cloak themselves.
8 And as the early presenter mentioned about using
9 samspace.org, that's not quite the effective mechanism
10 that it used to be, because it's becoming easier and
11 easier for people, if they are technically sophisticated,
12 to hide themselves.

13 MR. COHEN: Well, what are the harms to
14 consumers as a result of falsity in spam?

15 MR. PLANTE: I can answer that.

16 MR. COHEN: Yeah, you and Sam.

17 MR. PLANTE: Again, speaking from Symantec's
18 perspective --

19 MR. COHEN: Also to businesses.

20 MR. PLANTE: And to businesses in general. In
21 its most benign form, I think spam is just a heinous
22 inconvenience. I mean, certainly, any consumer can tell
23 you that getting a few e-mails once in a while that was
24 unsolicited might be annoying, but when you're starting
25 to deal with 50 to 100, and we are hearing of people that

1 are dealing with that type of numbers on a daily basis,
2 that starts to impact business productivity to the
3 individual employee. But when you're talking about some
4 of the subject matter in the content of some of these e-
5 mails, I mean, it smacks perhaps in some cases of sexual
6 harassing environment, work environment. There is some
7 question about that.

8 But then also the fact of the matter is that
9 there is a criminal association with some of the people
10 that are trying to get you to do something by opening and
11 acting on their spam that, again, a couple of years ago
12 didn't exist. We've talked to people that have again
13 tried to buy a Norton product that in fact was sold
14 through spam that have either got product that didn't
15 work and we can't support it, because we didn't sell it,
16 it's not our product, and about one out of ten tends to
17 sometimes share these e-mails are in fact credit card
18 scams. So, it's a wide problem, just on that one
19 experience.

20 MR. COHEN: Sam?

21 MR. SIMON: It's hard to over-state how, you
22 know, bothersome spam, per se, is to people now, and it's
23 not just bothersome. In fact, I would object to the
24 whole idea that spam is simply an innocuous inconvenience
25 to people to put up with. If it ever was, it is now much

1 more than that. It destroys the value of e-mail which
2 was and still is the killer app of the internet. It is
3 becoming virtually useless to many, many consumers.

4 The falsity of routing, per se, if we want to
5 just focus on that little bit, at one time in life, one
6 could spend some of their time to respond back and say
7 spam, go to samspace or find out who it is from and
8 notify their ISP, and you get a few pieces of spam and
9 you'd spend 15 minutes doing that. Now, it's just
10 impossible to do. Even if you could find it, it doesn't
11 matter, there simply isn't enough time in the day if
12 anybody cared to do that, and it ought not to be their
13 responsibility to have to do it. People want e-mail to
14 communicate with people and for reasons that they want
15 to.

16 Now, if you want to go to the -- and I'm not
17 sure -- on the simple mistitling of e-mail, I think that
18 that -- and we have -- had put a website called
19 banthespam.org or .com, asking people to submit to us
20 their experiences and how they'd been impacted by e-mail
21 and it -- you know, there's some really good stories that
22 we're getting and we have copies of that available.
23 People are -- again, I almost get emotional about it,
24 about the idea that you open a piece of e-mail because of
25 the wrong -- because of a header that has what would in

1 anybody's term be illegal pornography.

2 And I want to read just -- I have one comment
3 from some -- one of the comments from one of our people
4 who submitted a complaint. And it goes like this, "I can
5 no longer open my e-mail if any of my children or
6 grandchildren are now in the room. The so called junk
7 mail is more than anyone wants to deal with, but the
8 pornographic material is wrong. I choose not to buy
9 pornography for my home. I don't purchase pornographic
10 material to come in my mail. Why should I have to be
11 subjected to it in my e-mail? It should be my personal
12 choice and not forced onto my computer and into my home."
13 And it's from a grandmother who gave permission to use
14 her name, Mary Field.

15 This goes to not just the content but the fact
16 that she wouldn't know, when she opened it, inherently
17 what was in it. And, so, here is a person, a
18 grandmother, who says I can't even have children or
19 grandchildren in my room when I open my e-mail because
20 she has no idea inherently what's going to be in that e-
21 mail when they open it.

22 So, I think consumers are being damaged
23 enormously. In fact, the entire value of e-mail is being
24 weakened, if not destroyed, by not just the spam but the
25 way it's being done, that's the falsity of the

1 information.

2 MR. COHEN: So, that actually goes into what
3 was going to be my next question, which was how does the
4 falsity -- how is it affecting how consumers are viewing
5 the rest -- you know, all of their e-mail. And I think
6 you've spoken to that.

7 Chris, do you have anything?

8 MR. HOOFNAGLE: Sure, not exactly on falsity,
9 but I think the percentage of spam that we're seeing now
10 is pushing people out of participation in public fora,
11 and we're seeing so many commercial messages on the
12 internet that people are engaging in address concealment
13 and otherwise leaving public fora and speaking on ideas
14 of public concern because of the amount of commercial
15 speech that is out there that is suppressing it.

16 MR. COHEN: William, did you want to add
17 anything?

18 MR. PLANTE: Yeah, sure. Again, when we deal
19 with some of our consumer and our consumer complaints,
20 the first thing that we're concerned about again as a
21 corporation is the misuse of our name in advertising
22 product that in fact is not our product. You know, the
23 value of Symantec's name in terms of goodwill is in the
24 millions and millions of dollars, and when I have to --
25 not just write to individual consumers periodically,

1 because they have some virulent complaints, but to the
2 presidents of corporations who are enterprise clients who
3 want to understand why they're getting so much spam that
4 advertises our product, that's a very serious concern,
5 and that goes up to our boardroom, what are we doing
6 about it, are we diligent enough about it.

7 And, so, I have two different departments whose
8 responsibility is trying to fight both piracy and
9 counterfeiting, which is a problem, but also now spam. I
10 don't know that we're necessarily unique in that area
11 either. But then lastly, we've had to get to the point
12 of suggesting to people that they simply don't even open
13 up unsolicited commercial e-mail, that there's an
14 inherent danger to the point of, as the other speaker was
15 mentioning with the grandmother, that you can't open it
16 anymore without some fear of danger. And especially when
17 you're talking about some of the pornographic e-mail that
18 comes across.

19 I have kids, too, and they're not supposed to
20 get on my machine, but by golly, once in a while, you
21 know, it's a fast-speed machine and they're going to get
22 on it. And, so, yeah, not only just in terms of
23 consumers but for enterprise, for businesses, this has
24 been a real problem for us, and falsity is in so many
25 manifest ways a business threat and an affront to

1 individual morals.

2 MR. SIMON: Can I add something?

3 MR. COHEN: Sure.

4 MR. SIMON: There is the other part, there are
5 some commercial e-mails I would like to get. I mean, I
6 will occasionally sign up from businesses that I do team-
7 business with that I would like to be able to receive
8 that. And I think, not just me personally, but I think
9 other consumers it is an efficient way of communication;
10 it's a way to get specials if you're a good customer; and
11 by both the amount and the falsity and the distrust that
12 is created, it is making those legitimate uses of e-mail
13 by valid commercial enterprises less valuable and less
14 likely to be successful.

15 MR. COHEN: Do you see consumers being afraid
16 that the e-mail they're getting is, you know, somehow
17 false, sort of leaching over into other areas of the
18 internet, thus making them concerned about their personal
19 privacy or security in conducting transactions? Anyone?

20 MS. KOSCHIER: One thing that's come to our
21 attention, if I might jump in here, specifically the
22 forgery in the return path of the message oftentimes
23 leads to denial of service attacks for the legitimate
24 owner of that mailbox. If a spammer is initiating a spam
25 run and uses tmuris@ftc.gov in the return path of the

1 mail, like I just did, and half the recipients that he's
2 sending this spam run to are invalid, all that bounce
3 mail is going to go back to tmuris@ftc.gov.

4 We get phone calls on a weekly basis from
5 people saying I can't into my mailbox or our systems are
6 shutting down, please, help us out. It's a real big
7 problem. The consumer fears his safety. He wonders if
8 there will be retribution taken on him by parties who
9 think that he sent the spam in the first place. It's a
10 real concern.

11 MR. SIMON: We also have a second experience in
12 two weeks now where e-mail was sent out using a jacked
13 domain name, and it happens that it was advertising
14 Norton product, and this poor business -- in both cases
15 it was a relatively small business. They were saying I'm
16 getting all these returned e-mails and what's going on
17 here.

18 So, the first problem is you have a business
19 that starts being crippled and its own good name is
20 compromised because somebody's jacking their e-mail
21 address -- or, sorry, their domain name and spoofing off
22 e-mails. And it's pure profit for the Spammer that is
23 doing that. And then you get some guy who's got to tell
24 his client base that A, I didn't send this; and, B,
25 they've got to deal with all these returned addresses and

1 complaints. So, again, when we're talking about the
2 potential negative impact to businesses, that, from our
3 experience, is becoming an increased risk in using the e-
4 mail and the internet.

5 MR. SIMON: We actually have a real live person
6 who wrote and said that, "A Spammer recently sent out UCE
7 with forged sender information indicating that I sent
8 mail from a personal mail account I maintained. I
9 suffered a deluge wherein thousands of bounced e-mails,
10 death threats, complaints and removal requests in the
11 short span of time it took me to notice and disable the
12 e-mail account." And that was from David McKnett.

13 MR. COHEN: Thank you. Scott, do you have any
14 info on what percentage of spam is spoofed?

15 MR. RICHTER: I can really only speak on my own
16 inbox. Based on the spam I get, I'd say more than a
17 third. Unfortunately, there's no central clearing house
18 for e-mail, so, you know, I think the numbers are
19 unknown.

20 MR. COHEN: Is that consistent with your
21 experience?

22 MR. BELL: Well, our experience at MCI is it's
23 a higher number than that, probably 60 percent have
24 something that's forged in the actual headers itself.

25 MR. COHEN: Margot?

1 MS. KOSCHIER: It's difficult for us to
2 quantify -- to come up with a quantitative value for what
3 percent of e-mail is forged. I mean, considering we're
4 dealing with billions of messages a day. Really a lot.

5 **(Laughter).**

6 MS. KOSCHIER: Not an insignificant portion.
7 Enough to have a panel at the FTC consortium about it.

8 MR. COHEN: Well, and what are consequences to
9 a spoofing victim, other than the ones that we've talked
10 about?

11 MR. RICHTER: They need to notify the local
12 police authority if they're getting death threats, like
13 she just said occurred.

14 MS. KOSCHIER: Sometimes a campaign spoof that
15 is mimicking a legitimate click here to receive your
16 special offers or click here to get your instant greeting
17 from your friend, it leads to a web page, which this is
18 all spoofing, leads to a web page, which then downloads a
19 trojan or some such unknown executable onto this person's
20 computer, and then their security is really compromised.
21 Sometimes their personal information gets mailed out via
22 this automated program.

23 MR. SIMON: Well, just the problem with
24 spoofing is not only the person's e-mail spoof, but it is
25 part of this process by which you are encouraged to open

1 because you may be thinking you're getting mail from
2 someone you know or someone important or the Chairman of
3 the FTC, for example, and so it is part of what gets
4 people to open it. And that again means they're exposed
5 to information. Not just information, but potentially
6 dangerous or unwanted things that they otherwise wouldn't
7 even look at. So, it's both sides, not only the person
8 whose name or e-mail account's been expropriated, but
9 then the people who, because they think they know who's
10 sending it, are encouraged to open the e-mail.

11 MR. COHEN: Is there any legitimate reasons for
12 engaging in spoofing, trying to maintain anonymity?

13 MR. HOOFNAGLE: I wanted to address that point.
14 I think this is the main point I wanted to make today, is
15 that anonymity is a fundamental right tied to free
16 expression, the ability to participate in political
17 processes and the ability to share our ideas without
18 suppression from either public or private censors.

19 So, I think it's critically important that
20 people can still remain anonymous on the internet. So,
21 to the extent they are -- and send messages to people
22 without revealing their identity. I think we have to
23 remember that any model that we choose to take here in
24 the United States is likely to be copied in other
25 countries, as well. And if you take relative privacy out

1 of the internet, it will have substantial consequences
2 for those who live in countries without a First
3 Amendment, for instance.

4 But our country has a long history of
5 protecting anonymity in allowing individuals to engage in
6 deception when there are -- in their roles as speaking as
7 political speakers. And that tradition has been upheld
8 all the way through just last year, when Watch Tower
9 Bible was decided by the Supreme Court, which upheld the
10 right for individuals to go door-to-door pamphleting
11 about their religious beliefs in a community without
12 having to identify themselves first.

13 MR. COHEN: But you wouldn't use the same
14 criteria for commercial speech, would you?

15 MR. HOOFNAGLE: I think it's very important
16 that if you are to write legislation to somehow prohibit
17 the falsification of routing information that it not in
18 any way impinge upon political expression, and I think
19 we've seen a bill introduced -- excuse me, passed --
20 yesterday in Virginia that would prohibit those who send
21 over 10,000 messages with some type of falsification in
22 the header.

23 And I think we have to think very -- we have
24 to think very thoroughly over whether a law like that
25 could be applied to one of the very important list

1 servers that you or I might be one, whether it's David
2 Farber's list serve or Declan McCullagh's list serve.
3 These list serves have well over 10,000 members, and if
4 there is an ability to, let's say, post anonymously or
5 otherwise if there is some falsification in the header we
6 have to ensure that this political speech is not
7 prosecuted as spam.

8 MR. COHEN: I've had an e-mail request that the
9 speakers identify themselves when they answer our
10 questions, so if you could try and do that, I would
11 appreciate it.

12 I have a question for Margot and Bryan,
13 something we've been wondering about at the FTC. How do
14 Spammers select the domain names or e-mail addresses that
15 they will spoof?

16 MS. KOSCHIER: Okay, this is Margot. Sometimes
17 it depends on the weather; sometimes it depends on the
18 particular campaign they're engaging in. If they are
19 taking an actual product and spoofing it, they might very
20 well use the legitimate product's domain name or IP
21 addresses. It really depends on the type of Spammer.

22 MR. BELL: Bryan here. Our experience has been
23 it's one of two things. It's usually just randomly
24 choosing a domain; or we have actually seen Spammers go
25 after specific people and forge their domains for

1 whatever reason, most likely that they've made the
2 Spammer mad and are trying to get back at the actual
3 individual.

4 MR. COHEN: Other than the political speech
5 issue, I'm wondering whether there are any beneficial
6 purposes to allowing false routing or sender information.
7 Sam or William?

8 MR. SIMON: This is Sam. I can't think of one.

9 MR. PLANTE: I also agree. Absolutely no way
10 can this be a beneficial thing for businesses.

11 MR. COHEN: Should there be legislative
12 prohibitions on the forging of e-mail sender or routing
13 information?

14 MR. SIMON: I would fully support -- I thought
15 Senator Schumer made a really interesting set of
16 provisions, and I would definitely make it -- and being
17 focused and I appreciate the concerns about free speech,
18 and I think we do have to be careful, and I think the
19 best way to be careful is to aggressively eliminate the
20 amount of commercial spam, so it doesn't force more
21 Draconian measures.

22 But I think legislation -- I think the Federal
23 Trade Commission itself and just to remind TRAC and two
24 other consumer groups filed a petition in September of
25 last year. We believe the Commission could, on its own,

1 through enforcement, I believe it's filed a case against
2 a pornographer in which one of the grounds was the
3 falsity of the routing and spam. I think we need to go
4 after it aggressively now, not wait. The legislative
5 process can sometimes be delayed. The sooner you act,
6 the better.

7 MR. COHEN: All right, well, let me ask the
8 question the other way. Does anyone think there should
9 not be legislation prohibiting the forging of sending
10 false e-mail header information or routing information?

11 MR. PLANTE: Don't look at me.

12 MR. COHEN: Anyone. Just checking, no? Okay,
13 great. Anyone have any ideas what can be done to prevent
14 spoofing? Chris?

15 MR. HOOFNAGLE: I have an idea. It's actually
16 opposite of an idea to prevent. But, you know, year
17 after year in looking at privacy issues we see groups,
18 whether it's the government or in this industry
19 consortiums try to solve various problems on the
20 internet, whether it's spoofing, whether it's digital
21 rights management and copyright issues, whether it's
22 facilitating e-commerce or otherwise trying to accomplish
23 some business goal.

24 Every year we see a new idea of trying to
25 install a system of trust or the idea of a trusted sender

1 or a network of trusted senders. I think that would be a
2 bad way to try to stop spoofing and other types of fraud
3 on the internet, because it will subject us all to being
4 identified before we send e-mail.

5 MR. COHEN: Anyone else have any ideas?

6 Question for everyone. Is most spam -- we
7 heard Senator Schumer say that most spam is sent by a
8 small number of people. Is that actually true? Do we
9 have any information on that? Scott, do you have any
10 information?

11 MR. RICHTER: No, I was actually wondering
12 where he got that statistic from.

13 MR. COHEN: No? Okay. Here's a question that
14 we've been wondering about. What time of day or week is
15 most spam sent, and why?

16 MS. KOSCHIER: I actually have an answer for
17 that one. It's when we're not working. We find that
18 most of the -- with respect to how many recipients per
19 message arrive at our system, most of the high-recipient-
20 per-message mail is sent between the hours of 11:00 p.m.
21 and 5:36 a.m. in the morning, particularly heavy on
22 Fridays and weekends.

23 MR. SIMON: It's our experience that a lot
24 comes to people Sunday night. There is this phenomenon
25 of people showing up to work Monday morning and usually

1 the first thing they do is open their e-mail and look at
2 what came in and there is -- and this is almost
3 conventional wisdom in persuasion e-mail and non-
4 commercial e-mail that send out as to, you know, have it
5 sitting in somebody's e-mail Monday morning, because
6 that's when they're going to -- that's one of the first
7 things they do when they come to work.

8 MR. COHEN: Scott, when do you send most of
9 your --

10 MR. RICHTER: We've actually -- well --

11 MR. COHEN: Sorry.

12 MR. RICHTER: We've actually -- I mean, we have
13 some mail that goes at all different times, depending on
14 the customer's request, but we actually find that we have
15 better results if we send during the day than trying to
16 send in the middle of the night or, you know, different
17 hours.

18 MR. COHEN: Is there any cost factor that would
19 affect the decision as to whether to send it during the
20 day or at night?

21 MR. RICHTER: Basically we just usually leave
22 that up to the customer as to like what time they want to
23 send out.

24 MR. COHEN: Anybody else? Let's see. Anyone
25 have any idea what percentage of spam is now using

1 foreign servers? Does that seem to be a problem?

2 MR. PLANTE: Again, when we first started our
3 anti-spam program, we found a fairly even percentage of
4 U.S. domestic servers and foreign servers that were using
5 our product name. We're finding a shift in ratio, maybe
6 toward 60, 65 percent now, coming from foreign servers,
7 which from our perspective makes it much more difficult
8 to deal with when you're sometimes talking non-English
9 languages, and so it's much more problematic for us. I
10 think it's a shifting, at least in our experience higher.
11 William Plante.

12 MR. COHEN: Thank you.

13 MS. KOSCHIER: This is Margot. We've noticed a
14 trend recently where IP addresses that are registered to
15 entities overseas or domestic that have been dormant for
16 a while are apparently being misappropriated and borrowed
17 -- we're terming these zombie net blocks -- for spamming
18 uses. We're not quite sure how it's happening; we have a
19 couple of theories, but mail is coming from places where
20 it hasn't been coming from all along and these IP
21 addresses are somehow being routed by -- the routes are
22 being accepted by internet service providers, locally,
23 domestically, but the IP blocks a long time ago should
24 have been registered to folks overseas.

25 MR. COHEN: Could part of the problem be that

1 they've been sublet to other users?

2 MS. KOSCHIER: Could be, from what we've been
3 seeing; however, it would indicate that the owners of
4 these, the rightful owners of these net blocks, have no
5 idea that this is happening.

6 MR. COHEN: Scott, I have a question for you.

7 MR. RICHTER: Yeah.

8 MR. COHEN: I hope I didn't put you on edge.
9 Are senders of e-mail actually selling their own
10 products? Or do they send e-mails on behalf of other
11 clients?

12 MR. RICHTER: I think that would probably be
13 depending on each individual company that sends mail. We
14 have our own products, as well as we have customer
15 products, but we're mainly sending products on behalf of
16 our customers.

17 MR. COHEN: I've been asked to make sure that
18 everyone speaks in the mike when they respond.

19 Scott, in your experience, who writes the text
20 of the e-mail messages?

21 MR. RICHTER: Most of our advertisers have ad
22 agencies who do their ads for them and their credos.
23 They usually send over a couple different credos to see
24 which ones have better responses and different things
25 like that, but we usually leave that up to the

1 advertiser.

2 MR. COHEN: Does that include the subject
3 lines?

4 MR. RICHTER: Yes. We don't usually pick a
5 subject line for a customer; usually they'll give it to
6 us, what they would like to use with their ad. If we
7 find something that, you know, is inappropriate, we'll
8 notify them.

9 MR. COHEN: How do you determine what is
10 inappropriate?

11 MR. RICHTER: Basically we would look at the
12 offer and, you know, take it from a case-to-case basis.

13 MR. COHEN: So you actually look at the offer
14 and you look at the subject line and you look to see if
15 they're related?

16 MR. RICHTER: Correct.

17 MR. COHEN: And what happens if they're not?

18 MR. RICHTER: Then it's usually the job of the
19 salesperson to go back to the ad agency who sent us the
20 job and go over with them, you know, something that would
21 be more appropriate or, you know, something that we think
22 would, you know, work.

23 MR. COHEN: Do you have any experience with
24 others in the industry who might have different
25 practices?

1 MR. RICHTER: I -- you know, I have some -- you
2 know, I think I've read some stuff, you know, and I
3 probably, you know, from what I read on chat boards and
4 different things, but as far as the practices that we
5 follow compared to what another company does, I really
6 can't speak on their behalf.

7 MR. COHEN: Bryan, how many spam complaints do
8 ISPs receive every day?

9 MR. BELL: Well, from our experience it
10 averages about 7,500 complaints, and that is mass mail,
11 web packing and use-net complaints. Bryan Bell.

12 MR. COHEN: Margot?

13 MS. KOSCHIER: Millions.

14 MR. COHEN: Millions per day?

15 MS. KOSCHIER: Millions per day. This is a
16 good thing, though, because that means we know -- we know
17 what our members find objectionable and we can take
18 immediate action on it.

19 MR. COHEN: But do you find that with the spam
20 complaints you're receiving now that a lot of your
21 members are just clicking "notify AOL, this is spam,"
22 since that's the only option when they click that,
23 because there isn't a, you know, notify AOL, I just want
24 to unsubscribe because I'm 13 years old and my mom told
25 me, because she's read every day on the news and media

1 and ads that do not click on subscribe links?

2 MS. KOSCHIER: I think the button on the bottom
3 of the screen that says "report spam" is very clear that
4 it means report spam.

5 MR. PLANTE: Again, if I may for a moment.

6 MR. COHEN: Sure.

7 MR. PLANTE: William Plante here. About six
8 months ago, we started our spam watch at Symantec.com,
9 and after a few weeks we're getting maybe a couple
10 hundred, maybe 300 complaints in one day. And these are
11 e-mails from consumers that do not have any ability to
12 directly click a button and report this to us. They have
13 to find that e-mail address. As of Monday, we are now
14 averaging 1,500 to 1,600 e-mail complaints a day. Again,
15 that's just on our product-specific stuff, for people
16 that have to hunt the e-mail address down.

17 So, again, going back to some of the earlier
18 comments, I think that people are becoming more and more
19 frustrated and looking for ways to complain about it.
20 So, that's just been our experience. A lot more people
21 are becoming vocal about it.

22 MR. SIMON: And if I could add, this is Sam. I
23 think that most people don't -- you know, I think AOL's
24 button is great. I think most people, though, who are on
25 either a corporate or a generic e-mail service don't know

1 what to do; A, B, don't do it because it doesn't make any
2 difference. And, you know, I love the uce@ftc.gov where
3 I was for a while, but I gave up, because nothing
4 happened. You don't get a recognition, there's no sense
5 of results, and I think people just give up filing
6 complaints when there is no feedback or no impact of the
7 complaint being filed.

8 MR. COHEN: Well, the FTC receives, I believe,
9 170,000 UCE per day. It would be impossible for us to
10 respond to each one of them. We have over 11 million
11 spam in our spam data base. We do use the spam data
12 base. It is very important to us. We use it as part of
13 our investigations and it has been very helpful in
14 bringing a number of cases. So, I would, you know, urge
15 people to continue to forward their spam to the FTC.

16 MR. SIMON: I didn't mean it as a criticism as
17 much an indication that whatever reports going on is
18 probably only a small fraction of the actual feeling and
19 complaints that are out there.

20 MR. RICHTER: A big problem I notice is that as
21 an example, and they're not up here, but Yahoo several
22 weeks ago launched a contest and, you know, that the more
23 e-mail that you want to report as spam you'll be entered
24 to win prizes. And I believe that a lot of people are
25 reporting spam, or you know, that may not be spam,

1 because they're being enticed to do it. I personally
2 reported all my friends to try and win a free year of
3 Yahoo.

4 (Laughter).

5 MR. COHEN: You'll let us know if you win,
6 right?

7 MR. RICHTER: No, but, I mean, what I'm trying
8 to say is you can entice somebody and get -- I mean, if
9 somebody wants to report spam, I think that's great, they
10 should. But if you're promoting it as a contest or, you
11 know, as in a different way where it may be -- you know,
12 maybe they really did receive it, but unfortunately like
13 with somebody like Yahoo, there's no way to respond. We
14 don't know how many people click "this is spam" to enter
15 the contest. And maybe it isn't spam, how do -- you
16 know, and there is no way for us to respond and say no,
17 this is one you did opt in. This is one you did confirm
18 your e-mail address; this is, you know, when you visit
19 our website. There's -- and that's a big problem with
20 the industry, is that the people who send the mail don't
21 have those opportunities.

22 MS. KOSCHIER: I can tell you from experience
23 in looking at complaints that the marketing organizations
24 whose domain names reflect the information that's in the
25 headers do generate fewer complaints than those who have

1 anonymous information or random characters inserted into
2 the from addresses. The cleanliness of headers does make
3 an impact on how members view the mail.

4 MR. HOOFNAGLE: This is Chris from EPIC. I
5 think the ultimate enticement, I mean, aside from games
6 to entice people to report spam is actually to create a
7 law that has a private right of action so that
8 individuals can actually get satisfaction for spam. And
9 we currently have this framework in the telephone and
10 consumer protection act of 1991, a law that gives
11 individuals a private right of action in their local
12 state court, and there is an entire bar of people who
13 litigate under this law. And as a result, the junk faxes
14 and other annoyances that that law was designed to
15 prevent have gone down significantly.

16 MR. COHEN: A while back the FTC did a remove-
17 me surf, in which it found that 63 percent of unsubscribe
18 links did not work. My question is what percentage of
19 consumers actually try to unsubscribe from lists. Does
20 anyone have any information about that?

21 MR. RICHTER: Was that a -- when you say 63
22 percent of them didn't work, was that current e-mail you
23 received, or was that e-mail that you may have received
24 six months previously and, you know, an ISP decided to,
25 you know, terminate an account or -- I mean, there's -- I

1 think there are some issues or factors that could go
2 behind whether a remove address works.

3 MR. COHEN: That was within one to two months.

4 MR. RICHTER: Okay. And one thing that makes
5 it -- one thing that we've always done a good job of is
6 always making sure that each piece of e-mail that we send
7 has always a minimum of two ways to unsubscribe, usually
8 a web-based unsubscribe, as well as they can respond to
9 the e-mail with a remove. And we also have some where
10 we've experimented using call-in numbers or a postal
11 address, but, you know, basically the first two seem to
12 work the best.

13 Unfortunately, you know, there could be, you
14 know, instances where a black group, you know, tries to
15 do collateral damage or, you know, tries to force you off
16 an internet service provider's band width and it's, you
17 know, out of your control if removing doesn't work or
18 doesn't, you know, work for a period of time.

19 MR. COHEN: Do you test the remove links from
20 your e-mails?

21 MR. RICHTER: Yes. Yes. We'll add ourselves
22 to lists. We'll, you know, add two addresses, not
23 confirm one and confirm the other; you know, get two e-
24 mails, unsubscribe from one, make sure we don't get a
25 second one. We're constantly, you know, testing and

1 trying to do things that would, you know, ensure that
2 everything works.

3 MR. SIMON: This is Sam Simon. Part of the
4 problem right now is -- well, there are many problems,
5 but most -- one I would like to point out is that there
6 is a conflict of public information. If you watch a
7 typical consumer news show, a consumer reporter, they'll
8 do a story and say yeah, the remove things now do work
9 most of the time and it's an urban myth that they're
10 using this to harvest e-mails. And you'll turn to the
11 next station and it will give you the exact opposite
12 advice, that no, anytime you hit the remove me, that's
13 just a scam to show that you have a real e-mail address.

14 And consumers don't know what to do. Even if
15 yours worked, people don't know what to do, and by and
16 large, wouldn't dare use them because they're afraid that
17 this is testing the validity. But they get contrary
18 information. I don't think people know reliably what to
19 do about the remove buttons, to try them or not.

20 MR. COHEN: Is there any empirical evidence for
21 the proposition that by trying to remove yourself you're
22 actually confirming your e-mail address? Because that
23 has not been the experience of the FTC.

24 MR. RICHTER: No, that's --

25 MR. COHEN: We've actually tested for this.

1 MR. RICHTER: That's, I think, an urban myth.
2 I'm sure there was somebody who did that, but, I mean,
3 one thing like with us, as a practice we have, why would
4 you want to send to people who don't want e-mail? I
5 mean, that would be -- if somebody removes themselves from
6 your list, if they've joined your list and then they
7 remove themselves, it would seem unpractical to continue to
8 want to send to somebody like that.

9 MR. COHEN: Do you have -- while you're
10 speaking, Scott, do you have any information as to why
11 Spammers, not yourself, I'm not talking about you.

12 **(Laughter).**

13 MR. COHEN: Because I wouldn't call you that.
14 Why those people include removal links if they do not
15 work? What would be the purpose of doing that?

16 MR. RICHTER: You know, I would really have no
17 idea why they would. I mean, to me, like in most spam
18 that I receive, I don't ever see a remove link and, you
19 know, I mean, the less things in your e-mail I think that
20 you put, say, the word unsubscribe, remove and different
21 things, I think, you know, helps them to be filtering, so
22 I think it definitely plays against us by having two
23 remove links in every e-mail we send.

24 MR. COHEN: Do you think it adds to the
25 legitimacy of the e-mail if there's a remove-me link?

1 MR. RICHTER: Yeah, I think it's -- well, I
2 think the key -- things that make an e-mail more
3 legitimate, one is you send from a real domain name,
4 that's your domain; you get bounces, you're not -- you
5 know, nobody is going to get your bounce or it's not
6 spoofed or forged. Everybody, you know, anybody can
7 identify the information, the headers, as, you know, who
8 it came from.

9 MR. COHEN: Does anyone else want to speak as
10 to whether it adds legitimacy to the e-mail?

11 MR. PLANTE: Yeah, William here again with
12 Symantec. About three weeks ago, we had an incident that
13 involved a fellow who one of my investigators had direct
14 contact with and felt compelled to contact me on, where
15 he spent just over two hours going through all of the e-
16 mail filtering folder that he had and started
17 unsubscribing. And having done that, he was compelled
18 eventually to drop that e-mail address completely.

19 Now, that's anecdotally. I can't give you an
20 empirical statistic, but I can tell you that if the
21 choice is, you know, content filtering and sending the
22 stuff off to a folder and/or going up and opting out, I
23 would just as soon delete and try and deal with it in
24 terms of a volume problem every couple of days going
25 through a folder and deleting it.

1 This guy was just so distraught. He was
2 extremely angry. Not at us. And I can't even recall how
3 my investigator came into contact with him, but he was
4 looking for some help, and all we could ever tell him was
5 just delete the stuff, don't even open it, and we're
6 sorry to hear that it happened to you.

7 MR. SIMON: I actually have a real-life note
8 here, actually from Robert Helt, who's a senior technical
9 specialist, information system at General Mills, who said
10 that as a senior technical specialist in a Fortune 100
11 company I have seen the effect on productivity of
12 landslide of spam -- the landslide of spam has caused.
13 We tried to filter to block; changed e-mail addresses;
14 and various other countermeasures, but it still gets
15 through. Trying to, quote, opt out, or quote,
16 unsubscribe, just makes it worse.

17 MR. COHEN: Are there any questions from the
18 audience? Lots of questions from the audience.

19 **(Laughter).**

20 MR. COHEN: Brian?

21 MR. HUSEMAN: I wanted to follow up on one
22 thing. Excuse me. AOL tells its members to not
23 unsubscribe from e-mail, in AOL 8.0. And I was just
24 wondering what your basis for telling your members that
25 was.

1 MR. COHEN: Margot, will you repeat the
2 question?

3 MS. KOSCHIER: The question was we allegedly
4 instruct our members not to attempt to unsubscribe
5 themselves from e-mails. And that is not true. At
6 keyword postmaster or keyword mail controls, I believe
7 keyword post -- actually, it's keyword junk e-mail now,
8 we say look at the e-mail, treat it suspiciously, if you
9 believe that your unsubscribe request will be honored, by
10 all means, go ahead and unsubscribe. If you have any
11 doubt, don't. We leave it to the member to decide.

12 MR. COHEN: Gentleman in the back? Please
13 identify yourself.

14 (Question not audible from audience).

15 MR. COHEN: So, the question -- the point was
16 that web bugs might be contained on HTML pages and that
17 by opening up the link or the message that's in the e-
18 mail, it sends back a notification that the e-mail
19 address is valid.

20 Gentleman here.

21 AUDIENCE MEMBER (Partially audible): The
22 question I want of the panel, my company sends
23 permission-based e-mail on behalf of our members, so in
24 the e-mail headers, we will actually have the return
25 address of our member who's sending it or whom we are

1 sending it on behalf of; however, on the e-mail headers,
2 it will show our IP address as the originating e-mail
3 server. Would that be considered false --

4 MR. COHEN: So, the question is when you're
5 sending e-mail on behalf of your marketers, the
6 information shows that it is coming from you when it
7 actually might be coming from someone else. Is that
8 correct?

9 AUDIENCE MEMBER (Partially audible): -- it has
10 our member's return address in it.

11 MR. COHEN: Oh, it has your member's return
12 address?

13 AUDIENCE MEMBER: Right, if it is coming from
14 them. We are just sending it for them.

15 MR. COHEN: Okay.

16 AUDIENCE MEMBER (Partially audible): The e-
17 mail itself is coming from our servers; however, we put
18 the member, our member's e-mail address in the from line.

19 MR. COHEN: So, if we were tracing it, it would
20 come back to your server.

21 AUDIENCE MEMBER: Yes.

22 MR. COHEN: But if we looked at the e-mail --
23 the IP address on the e-mail, it would have somebody
24 else's server.

25 AUDIENCE MEMBER: -- first return address is

1 his machine.

2 MR. COHEN: Right.

3 MR. SIMON: Well, TRAC in this position -- it
4 would be my position that the real party in the interest
5 of any commercial e-mail should be identified correctly.
6 And it doesn't really bother me where it might be, but if
7 it were in the text of the e-mail, with a valid phone
8 number, as well as e-mail address, that would be enough
9 for us.

10 MR. COHEN: Please introduce yourself.

11 MR. SCHOKEL: I'm Brad Schokel (phonetic) with
12 AAC&G.org, which is our user group association of
13 computer users. One of the questions I'd like to address
14 would be the validity of the unsubscribe address. I'm a
15 member of the task force that analyzes spam, we have been
16 for several years now. And when we test the -- I don't
17 know how FTC tests it, other than sending mail to them,
18 but we also looked them up in the WhoIs and called the
19 telephone numbers and then called the city where they
20 reside and so forth.

21 And the big problem we found in the way we
22 separate it out, who might be a valid unsubscribe address
23 and who might not be, which who hasn't falsified their
24 whois information? And generally speaking, we're only
25 finding 17,000 pieces of spam we analyzed, there were

1 like 37 which were valid. Okay? And the thing of it is,
2 when you go back to the whois, that's really the only way
3 is the owner of the domain. And most of those are either
4 rows of Xs or they're completely erroneous telephone
5 numbers, like to a vacant lot in New York, something like
6 that. And, so, that's really the only way you have to
7 track back the owner of that domain.

8 The other thing I'd like to address, too, is
9 the foreign ports thing. There seems to be a disparity
10 in data or people not understanding the percentages on
11 that. But that is like doubling every two or three weeks
12 -- (inaudible). And in terms of identifying 150, what
13 the Senator was talking about, there -- I think he has
14 really accurate information. We actually have about 225
15 IP blocks who consistently send spam, but through our
16 network off other user groups who have their own mail
17 servers, who are sending their logs, we've analyzed logs
18 from all over the country. It seems like no legitimate
19 mail is coming from these numbers. So, it's sort of like
20 if they're only serving spam and there's no legitimate
21 mail -- (inaudible) -- then they have to be Spammers.

22 MR. COHEN: Okay.

23 BRAD SCHOKEL: I only wanted to make that
24 point.

25 MR. COHEN: Thank you. The issue -- it's a

1 very interesting point about comparing the whois
2 information to the unsubscribe information. About a year
3 or so ago the FTC sent a letter to ICANN and it's the
4 Bureau of Consumer Protection, I believe, recommending
5 that the whois information should be accurate, because
6 consumers rely on that information and it is important
7 that the information be accurate. And this shows why.

8 AUDIENCE MEMBER: They just passed an
9 initiative, too, just about two weeks. They finally
10 passed an initiative at ICANN to cause registrars -- we
11 need somebody here from ICANN. Is anybody here from
12 ICANN?

13 MR. COHEN: All right, well --

14 AUDIENCE MEMBER: Have the registrars check
15 once a year the validity, and if it's not valid, they
16 block that domain.

17 MR. COHEN: Thanks, Mona.

18 MR. RADEN: Some of the leading e-mail software
19 packages now have preview panes in which they actually
20 open up the e-mail for you automatically, if you will.
21 Now, if web bugs are, in fact, one of the ways that they
22 validate your addresses, is there anything, short of
23 closing the preview panes, that the consumer can do, the
24 recipient can do? And I'm David Raden from the Post
25 Gazette and Megabyte Minute Radio.

1 MR. HOOFNAGLE: I think there is. There's
2 filtering you can do to disable HTML as you receive it in
3 your mailbox. I don't want to promote certain products,
4 but I think it's worth looking at Spam Assassin and some
5 of the front-ends for that program that will turn off
6 HTML e-mail.

7 And some spam software itself will let you
8 disable spam -- excuse me -- some e-mail software itself
9 will let you disable HTML as you receive --

10 AUDIENCE MEMBER: (Inaudible) -- using the
11 product itself that you know of, short of shutting down
12 the -- (inaudible).

13 MR. HOOFNAGLE: I don't know the whole line of
14 products well enough to answer that question.

15 MR. COHEN: Would the panelists say it is
16 deceptive for a remove-me link to take the recipient off
17 of only the list for that mailing, rather than from the
18 list for all future mailings?

19 MS. KOSCHIER: I would think it would depend on
20 what the remove-me link were advertising it would do.

21 MR. COHEN: Scott, do you have anything?

22 MR. RICHTER: I didn't really understand -- I
23 mean, as far as remove them from the -- are you saying
24 remove them from one e-mail or remove them from all
25 future e-mails?

1 MR. COHEN: Remove them from one e-mail rather
2 than all future e-mails?

3 MR. RICHTER: Why would they --

4 MR. COHEN: Would that be deceptive?

5 MR. RICHTER: Oh, I mean, anybody who clicks --
6 yeah, to me, yeah, and anybody who clicks with us would
7 be removed from all future e-mails.

8 MS. FLANAGAN: Hi, my name is Erin Flanagan,
9 I'm with Consumer Base. Everything that we were talking
10 about or you were talking about in this panel is clearly
11 fraudulent with forging headers and open relays and
12 everything. And I never hear any distinction between any
13 commercial -- like legitimate commercial marketers and
14 like fraudulent Spammers. And I feel like commercial
15 marketers are constantly being grouped in the same
16 category, but I don't think that we do anything
17 fraudulent, yet we get treated like some porno Spammer.
18 So, how are you ever going to differentiate between a
19 legitimate marketing company and some spam operation out
20 of somebody's basement?

21 MR. COHEN: The question is how does one
22 differentiate between commercial -- legitimate commercial
23 e-mailers and Spammers.

24 MR. SIMON: This is Sam. I think my point
25 earlier is that legitimate companies are among those who

1 are hurt the worst by this kind of spam, so you're
2 endorsing effective remedies, banning together to get
3 something done quickly would be a way to help yourself,
4 A; B, there are a variety of viewpoints on whether there
5 ought to be only opt-in. But assuming that there isn't
6 an opt-in world, that it is an opt-out, I would say, and
7 it is our view and the petition our group's filed would
8 expect that any legitimate e-mailer would have an
9 accurate description of the e-mail on the subject matter;
10 an accurate identification of who sent it; how to reach
11 those people in real time, as well as a valid unsubscribe
12 element, all of that before we would consider it a
13 legitimate marketing piece.

14 MR. PLANTE: William here with Symantec. Let
15 me make one other point, that with our resellers and
16 redistributors of our product, we have had discussions
17 with them about the use of e-mail as a marketing tool,
18 simply because we've been dealing with the spam problem
19 now for several months, well, six months, actually,
20 approximately. And it is so tainted, that mechanism,
21 that medium, that although we don't have a contract with
22 them, so they can't, but, you know, by verbal agreement
23 they've acknowledged that they simply can't use it
24 anymore because there's no validity to it.

25 MS. KOSCHIER: From an AOL perspective, I can

1 say that our determinations as an organization of which
2 entities are Spammers and which are not, regardless of
3 whether or not you consider them to be sketchy are based
4 on what our members decide. It's complaint-driven in our
5 perspective.

6 MR. COHEN: Okay. Sorry, go ahead.

7 MR. NOONAN: My name is Kevin Noonan, I'm the
8 Executive Director of the Association for Interactive
9 Marketing, and I just wanted to say that we've been
10 working with a lot of these ISPs, and I believe that AOL
11 and a lot of them are doing a great job in trying to
12 combat this.

13 I also wanted to congratulate CNET, who I
14 receive e-mails every day from, and sometimes don't open
15 them for a period of a week or two, and after about a
16 two-week period, my investor CNET newsletter wasn't
17 opened, and they actually sent me another e-mail saying
18 we've noticed that you haven't opened this for some time,
19 do you wish to remain on our subscribe list, and if you
20 do, then just let us know, and if we don't hear from you,
21 we'll take you off that list. And I think on the other
22 side of the fence, that's a very positive thing to do.
23 And my question would be to the panel, is there any
24 evidence of the newer TLD, the top-level domains, of
25 being more egregious Spammers than the dot-coms out

1 there.

2 MR. COHEN: The question is whether there's any
3 evidence that the new TLDs are more egregious Spammers
4 than the dot-coms. Anybody have any experience?

5 MR. SIMON: But there is so much. I mean,
6 actually, there is so much out there and so frequent that
7 it would be very hard to make that kind of judgment.

8 MR. COHEN: Questions? Anyone?

9 MS. LIEB: Rebecca Lieb with Internet.com. I
10 wanted to make, if I may, two additional points on two
11 items that were discussed during this panel that I think
12 were perhaps overlooked. One was the material damage of
13 spoofing to businesses. There was some discussion of
14 brand and reputation damage. I think it's important to
15 note that a number of companies have had to shut down
16 operations or at least the IT aspect of their operations
17 for several days in some instances after being bombarded
18 by bounces and by complaints, effectively putting them
19 out of business.

20 Secondly, on the unsubscribe, we've been
21 hearing a lot about unsubscribe links in e-mail, but
22 that's not necessarily been clarified. Sometimes
23 unsubscribe links take you to a landing page where you
24 can unsubscribe or you're automatically unsubscribed.
25 But very often these links are in e-mail that

1 unsubscribes the address from which the e-mail was sent.

2 When e-mail addresses are illicitly harvested
3 off websites, lots and lots of aliases are harvested
4 along with them. Feedback@, webmast@, abuse@. Very
5 often these aliases are distributed to dozens of people,
6 none of whom can send an e-mail from that address to
7 unsubscribe from anything they were subscribed to, which
8 means a lot of stuff is effectively unsubscribable, given
9 the current form.

10 MR. FOX: Jeff Fox, Consumer Reports. I just
11 want to submit a little bit of evidence about the
12 unsubscribe option. About 14 months ago, which I now
13 regard as the good old days when most of our spam did not
14 have forged headers, that's how much it's changed, I
15 think, in the past year, we did a little experiment with
16 some of the spam we were getting, repetitive spam coming
17 from the same domains. And we unsubscribed to a couple
18 dozen of them.

19 We published this about a year ago. Most of
20 them stopped coming, you know, within a couple of weeks
21 after we unsubscribed. But we noticed a few weeks later,
22 some new e-mail started coming from domains which when we
23 did a whois, coincidentally, happened to have the same
24 registration address as some of the domains we'd
25 unsubscribed from.

1 And, so, you know, nowadays with forged
2 headers, this whole thing may be pointless, you may not
3 be able to trace it anymore, but this was some evidence
4 that the same companies would apparently unsubscribe you
5 from, you know, It's-Amazing-Offers.com, or Big-Deals-
6 For-You.com, and then, you know, a month or two later --
7 and the registration address of the new domain was often
8 quite recent, and so for 10 or 20 bucks they can just
9 take out a new domain. They can claim to be respecting
10 your unsubscribe, and then if you don't know how to do a
11 who is, you know, there they are Spamming you again under
12 another name. So, this is some of the practices that go
13 on.

14 MR. COHEN: One more question. Someone over
15 there.

16 AUDIENCE MEMBER (Partially audible): Hi, I'm -
17 - (inaudible) -- and I'd like to return to the question
18 of anonymous speech. I get a lot of anonymous mail from
19 deliberate anonymizing services. The best known is --
20 (inaudible) -- but they're all over the place. And what
21 the headers in those messages say, this mail came from
22 IT, we don't know where it came from before that, because
23 we deliberately didn't record it. It seems to me that's
24 a perfectly reasonable way for people who want to provide
25 anonymous service to provide it. (Inaudible) -- I don't

1 see anything that's forged in that. I wonder whether the
2 lawyers here would agree that this is -- it is possible
3 to have mail that is anonymous without any kind of
4 forgery.

5 MR. COHEN: Chris, do you want to respond?

6 MR. HOOFNAGLE: I'd like to speak about that.
7 I mean, there are several different types of anonymous
8 re-mailers, and I'd have to think about whether there
9 could be -- whether what you say could be written into a
10 law so as to affect the commercial senders and not affect
11 the sending e-mail over the re-mailer. But I'll have to
12 think about that.

13 AUDIENCE MEMBER: Well, a related question is
14 is there such a thing as anonymous commercial speech? I
15 would say that a business -- that the point of commercial
16 speech is to get somebody to contact you and buy
17 something --

18 MR. SIMON: This is Sam. I wanted to come back
19 to that topic briefly, too. And I would first, on your
20 point, I wouldn't think there's any valid anonymous
21 commercial speech. I do think that the remedies are
22 sensitive, and I think the idea of basing remedies simply
23 on the numbers of e-mails are of concern, because there's
24 -- increasingly e-mail is trying to be used in our
25 political system, not just in advocacy, but if you -- as

1 we go into the next few presidential campaigns, you're
2 seeing increasing numbers of both parties and candidates
3 using, and if our test of what becomes spam --
4 unsolicited commercial e-mail is speech from political
5 candidates, I think that that's a problem, and therefore,
6 I think the solutions are difficult, although I think
7 that aggressive prosecution, and I like the criminal
8 prosecution piece of this, is important, it will
9 hopefully scare away the worst offenders.

10 MR. COHEN: And we will have to end on that
11 note. Thank you very much. We have a 15-minute break.

12 **(Applause).**

13 MR. FRANCOIS: We're going to go ahead and get
14 started. This is panel number four of the day, dealing
15 with open relays, open proxies and formmail scripts. We
16 have a distinguished panel with us here today, and
17 instead of two hours, we're going to hold it to about an
18 hour and 45 minutes and reserve questions until the end.

19 Briefly, what this is about is we will discuss
20 open relays and proxies, but in general, this deals with
21 security issues where people who don't have the intention
22 of sending voluminous amounts of spam to people actually
23 end up sending voluminous amounts of spam to people.
24 And, so, this is a topic that really touches on not just
25 businesses that receive it, but businesses that may have

1 their systems that are not properly configured;
2 individuals who maybe have home networks that are not
3 properly configured, which allow Spammers to really
4 manipulate the system to their advantage to, one,
5 facilitate sending a large amount of e-mail messages
6 without -- at no cost, but also allowing them to displace
7 the burden and any type of adverse impact on people that
8 have these security weaknesses.

9 So, we're going to jump around a little bit.
10 We have several -- three presentations for you. One will
11 be of open proxies; the other will be of open relays; and
12 the final presentation, which will be at the end of the
13 panel, will talk about new threats, new and emerging
14 threats to security and which Spammers can exploit.

15 Then beyond that, after we do our first two
16 demonstrations with proxies and relays, we will have a
17 discussion about open relays, open proxies, honeypots,
18 the international aspects of open relays and open
19 proxies, new and emerging threats, as well, and then we
20 will save some time for questions from the audience.

21 So, with that in mind, I will defer to our
22 first panelist, Matt Sergeant from MessageLabs, who will
23 give us a very brief presentation about open proxies.
24 And then we will move to a PowerPoint presentation by
25 Nick Nicholas, which will be addressing open relays.

1 After that, we'll jump into a general discussion of both
2 open relays and open proxies.

3 MR. SERGEANT: Hi, I'm Matt Sergeant, the
4 Senior Anti-Spam Technologist for MessageLabs. What I
5 want to talk to you all about today is the problem of
6 open proxies. And first of all, I want to really explain
7 in very simple terms what an open proxy is, because this
8 is a fairly recent threat that most people who deal with
9 spam have dealt for a long time with the problem of open
10 relays. And as such, the problem of open relays has been
11 communicated extremely well to the general public, but
12 perhaps a great number of people don't really know about
13 the growing problem of open proxies. So, I want to
14 explain today about how they work and why you might have
15 one.

16 The picture here is to basically show that
17 somebody at home might install a DSL connection, so
18 they've got a permanent line to the internet, they've got
19 a high-speed connection. And one of the things that
20 we're seeing more and more of in recent times is that
21 people want to build an internal network, and for this
22 internal network, they want the other computers that they
23 buy to be able to access the internet to browse the web
24 and receive and send e-mail.

25 The thing about doing this with the regular

1 home DSL subscriptions is that the computer that you get
2 that connects to the internet gets a public IP address,
3 but the computers on your internal home network get a
4 private IP address. So, here we've got a setup with
5 three computers, one connected to the internet with a
6 public address and two behind the internet connection
7 with private IP addresses. And those two computers can
8 communicate with each other within their own internal
9 network, but by default, the usual situation is that they
10 can't browse the web.

11 So, the person setting up this might go to
12 google, usenet and type in how do I, you know, connect
13 these computers to the internet? How do I get them to
14 browse the web? And one answer that might come back
15 would be to install a proxy server. So, they do this and
16 they install the proxy server and now, by doing this, the
17 computers behind the internal network can browse the web
18 and use e-mail. So, that seems like a great situation
19 for the person who's just created their home network.

20 But what they don't realize often is that these
21 proxy servers are created in an insecure manner. They're
22 installed by default open, so that the entire world can
23 come in and use this proxy server to connect to the rest
24 of the internet from that one connection. So, the
25 Spammer or potential abuser, because this is not just a

1 problem for Spammers, open proxies are a source of
2 various kinds of abuse, they come in, they connect to the
3 proxy server installed behind somebody's DSL connection,
4 and from that point they can browse the internet. And
5 the reason that they do this is simply to hide where
6 they're coming from.

7 The other reason that Spammers might do this is
8 because there are a large number of these open proxies
9 out there, so they can use this as a system whereby they
10 can hop around all over the place, sending 100 e-mails
11 from one, 100 e-mails from another and hopping around as
12 quickly as possible. And they do that so that their
13 source of e-mail doesn't get noticed. So, 100 e-mails
14 from one particular host might quite easily fall under
15 the radar and not get noticed by an incoming mail server.
16 Whereas, you know, the total volume that they're sending,
17 which might be millions of e-mails, certainly would get
18 noticed. So, this allows them to hide and sneak around.

19 The way to secure an open proxy is very simple.
20 You can either install a firewall or you can change the
21 configuration of these proxy servers. It's as simple as
22 that.

23 The problem with open proxies, though, is that
24 unlike open relays, the owner of the open proxy never
25 finds out that they have an open proxy. The machine

1 running the open proxy is not really designed to send e-
2 mail in the same way that an open relay is. When you
3 install an open relay, it's designed to be a mail server,
4 so you expect to be sending mail out from it. And if
5 that server ends up in an IP black list, you find out
6 about it very quickly, hopefully, and you can do
7 something about it.

8 With an open proxy, it's not designed to send
9 e-mail, you just -- the DSL connection would mean that
10 you are supposed to send e-mail through your ISP. So, if
11 you had, for example, a Roadrunner connection, you would
12 go through Roadrunner's SMTP servers, rather than sending
13 direct to the recipient.

14 So, the owners of those open proxies, they
15 don't get to find out that they've been blacklisted.
16 They don't get to find out that they have an insecure
17 system, so they can't fix them.

18 The other thing is that ISPs don't check these
19 blacklists, so they have no way to detect whether their
20 own customers have actually installed an open proxy.
21 They -- most ISPs still aren't doing scanning of their
22 customers to find these things, so they just -- they get
23 set up and then they just remain there. So, the number
24 of these open proxies is still on the increase. It's
25 rapidly increasing. I think the number of open proxies

1 is doubling about every five or six months at the moment.
2 So, it's a real problem.

3 Logs are nonexistent for these. They are home
4 users. So, if you have a source of spam coming through
5 an open proxy, you can find out the IP address of the
6 open proxy, find out that it is an open proxy, but you
7 can't find the real Spammer behind that, the Spammer's
8 actual computer, because it's very difficult to go to a
9 home user and say give me the logs. You know, it's much
10 easier to go to a mail administrator and say that,
11 because they would have procedures in place for
12 maintaining those logs and backups and things like that,
13 whereas a home user doesn't maintain that kind of thing
14 and they will very often delete logs, reformat their hard
15 disk and things like that.

16 And the final point is that end-users, they're
17 really not sys-admins at the end of the day. So, they're
18 not really that interested in fixing these problems. If
19 you contact these home users and say excuse me, you have
20 an open proxy installed on your system, they'll be like I
21 don't know what you're talking about, because they don't
22 really understand the problems here.

23 So, how does an open proxy work? I was
24 actually going to try and do a demo of this, but the
25 internet connection is not very good, so I'll just talk

1 through it. It's very, very simple to abuse an open
2 proxy. Most of the spam-sending ratware out there now
3 incorporates features to use open proxies directly. But
4 from a very sort of low level, all you do is telnet to
5 the open proxy on the port that the proxy is listening
6 on, and you type connect and here I'm connecting to
7 mail25.messagelabs.com, which is one of our mail servers,
8 connecting to port 25, which is SMTP servers, and then
9 you press return twice. And if you get a response from
10 that that says 200 connected, which is the response you
11 would get from an SMTP server if you successfully connect
12 to it, you're free then to send e-mail direct to that
13 SMTP server.

14 So, this is an incredibly simple way of doing
15 abuse. There are a number of different types of open
16 proxies which work slightly differently, but the premise
17 is basically the same, and the software that is used to
18 send spam wraps all of this up. So, you don't actually
19 have to -- as a Spammer, you don't have to manually type
20 any of this is, it's all done automatically for you.

21 And the final point there is that the IP
22 address that you might be using to abuse the open proxy
23 will not show up in the headers of the e-mail that gets
24 received. So, it's a completely anonymous service that
25 happens here.

1 How many open proxies are out there is a very
2 difficult figure to try and estimate. We think at the
3 moment there's somewhere in the region of 52-hundred-
4 thousand. It seems to be a vaguely agreed-upon figure in
5 the community. At the moment, as far as quantity of spam
6 is concerned, last month in March we were seeing about 60
7 percent of all our incoming spam coming through open
8 proxies. So, this is a huge chunk of the spam problem
9 right here.

10 And the use of open proxies is increasing all
11 the time. It's probably up to something like 65 or 70
12 percent for April.

13 How do Spammers find these open proxies? Two
14 ways really. They will actually go out and they will
15 port-scan IP addresses in networks that they know host
16 DSL connections. So, they will go out to the Brazilian
17 ISPs, who they know that they -- you know, they have
18 these DSL connections and a lot of their users aren't
19 terribly knowledgeable. They will go out to all the
20 major U.S. ISPs who give out DSL connections.

21 And they will actually scan for them using
22 specific software designed to find these proxy servers.
23 And very much like we saw earlier in the demonstration of
24 e-mail harvesting, you just get a list of these, which
25 you can then plug into the ratware to send your spam out.

1 The second way is that some of the commercial
2 ratware on the internet which you can pay for comes with
3 a monthly subscription that you pay for and the provider
4 will send you either monthly or weekly a predetermined
5 list of open proxies that you can abuse. And this
6 installs direct into the client, it's completely
7 automated, you don't have to do any of the scanning
8 yourself, and obviously it is a very powerful tool for
9 anonymizing the e-mail for the Spammers.

10 Finally, how do we fix the problem? A big part
11 of the open proxies problem is getting ISPs to take
12 action for their customers. They -- we believe that ISPs
13 need to start scanning their customers, finding out if
14 they have these insecurities and getting their customers
15 to fix the problem, and if they can't -- if they can't
16 get the user to fix the problem, they really should be
17 disconnected from the internet, because they are
18 inflicting this abuse on the rest of us.

19 And the quote there is, you know, we don't want
20 to drink their dirty water anymore; we'd rather they
21 cleaned it up before inflicting it upon us.

22 Another thing that ISPs can do is they can
23 check the public blocklists against their IP ranges, so
24 they can go through these blocklists and say, do I have
25 any customers listed in your blocklist, and if so, they

1 can then find out who the customer is and get the problem
2 fixed.

3 And finally from a receiving end point of view,
4 for those of us receiving spam, use of these DNS
5 blocklists is extremely effective now against the spam
6 problem. The open proxy blocklists are very targeted
7 toward open proxies, and as such, they're very effective
8 and have very, very low false positive rates, so that
9 they're very useful.

10 And, finally, a question mark, because there
11 are probably multiple solutions, and hopefully we can
12 discuss some of those.

13 Do you want me to go and talk about formmails
14 right now?

15 MR. FRANCOIS: Yeah, so that way the -- we can
16 have a chance to switch the computers.

17 MR. SERGEANT: Okay.

18 MR. FRANCOIS: We're going to have Matt talk
19 about formmail scripts and the inherent weaknesses in
20 those that Spammers use, have used and exploited to send
21 their spam.

22 MR. SERGEANT: Okay. I just knocked up one
23 slide about formmail scripts. Formmail scripts actually
24 aren't used very much in spam any more. They have
25 seriously declined in popularity. We still see every now

1 and then some spam coming through that has abused a
2 formmail script, but it's very much on the decline.

3 The formmail scripts are very simply scripts
4 that have been downloaded from the internet for the
5 purpose of building feedback forums on web pages. So,
6 you would have a form on the web page that says please
7 fill in your details and click submit and we'll send you
8 some more information. And many websites have these kind
9 of things.

10 The most common one that people have download
11 is the one from Matt's Script Archive, called
12 formmail.pl, and that's not me by the way, that's a
13 different Matt. This script was originally developed
14 around 1996 and was very insecure by default. It allowed
15 people to come into the web page and send almost any
16 content that they wanted through that script. So, you
17 could -- this is another thing, very much like open
18 proxies, a way to anonymize yourself so that it looks
19 like the e-mail is coming from somewhere else.

20 The problem now has been mostly fixed. If you
21 go now to the web page for Matt Script Archive, it says
22 there are some security problems with formmail.pl and we
23 recommend that you use the NMS version of this script.

24 So, there's a website there which seems to have
25 faded out a bit in the presentation, but it's nms-cgi.

1 sourceforge.net.

2 And these are actually a bunch of friends of
3 mine in London who sat in the pub one day and said you
4 know, we're really sick of hearing about this formmail
5 problem, let's fix it, let's get together and fix it.
6 So, they've provided free equivalents that are secure by
7 default for the formmail scripts and various other of
8 Matt Scripts. So, you can go there and download that and
9 fix the problem.

10 And that's about it for the formmail scripts.

11 MR. FRANCOIS: Thank you, Matt. Just a quick
12 question, in terms of while this may not be a method that
13 Spammers are using frequently, are there still -- what's
14 the prevalence of the formmail scripts that are corrupted
15 that are still out on the internet? Do you have any idea
16 of what that might be?

17 MR. SERGEANT: It's a very difficult figure to
18 test for. It seems that there have been a large number
19 of downloads of the NMS equivalent, so hopefully the
20 insecure ones are going away. I can't give you an exact
21 figure, unfortunately.

22 MR. FRANCOIS: And maybe you can briefly kind
23 of go into a little detail in terms of what was the
24 specific problem with the formmail scripts that were
25 being exploited.

1 MR. SERGEANT: Okay. The specific problem with
2 formmail scripts was that the recipient e-mail address
3 for where the contents of the form were to be sent was
4 encoded directly in the web page. What this allowed is
5 the -- somebody abusing the formmail script could
6 construct their own web page containing a completely
7 different recipient and a completely different set of
8 content and post the results of that form through the
9 script. And that would send all of that content to the
10 falsified recipient and it would appear to come from the
11 formmail web page.

12 MR. FRANCOIS: Was there any problem with Send
13 Mail or Send Mail 8.8 or that's involved in formmail or
14 is that another problem that I'm thinking of?

15 MR. SERGEANT: It's possibly another problem
16 that you're thinking of. There was a slight -- there is
17 a very small issue there in that Send Mail allows you to
18 do routing based on the -- a specific formatting of the
19 e-mail address. And, so, when this issue first cropped
20 up, Matt fixed the problem in formmail.pl, or so he
21 thought, but it still allowed you to do what's called
22 percent routing.

23 MR. FRANCOIS: What is that, if you could
24 explain that a little bit?

25 MR. SERGEANT: It's a way of formatting an e-

1 mail address recipient. So, you say -- you can say that
2 the recipient is supposed to be map%messagelabs.com@, and
3 then the server. And Send Mail, although it looks like
4 it should be going to a different server, Send Mail will
5 kindly route it to the domain after the percent sign.
6 So, formmail did a very simple check to see if the domain
7 was in a valid list of domains, but it didn't check for
8 the percent routing problem.

9 MR. FRANCOIS: All right. Now we're going to
10 turn to -- jump out of water a little bit -- and turn to
11 Michael Rathbun, who is with Allegiance Telecom in Texas,
12 and to give us an overview of the arms race, so to speak,
13 in spam, and where -- how we got started and where we are
14 today and how we got there. We're going out of order,
15 just to kind of give the computer folks a chance to
16 change the computer so we can do the other demonstration,
17 so that's why we're going out of order.

18 But, Michael?

19 MR. RATHBUN: Thanks, Renard. In 1995, I first
20 encountered internet e-mail spam as a problem when it was
21 being sent by a fellow in Seattle named Willie Newell
22 (phonetic). And Willie had a product to sell that later
23 had some suitability issues, but he basically buried
24 anybody who was posting to usenet in those days with spam
25 for the Zygon learning machine. And you might call him

1 the first large-volume but rather naive Spammer because
2 he sat essentially on a T1 line, dedicated connection, to
3 an ISP in Seattle and he sent out quite a bit of mail.

4 Well, the first thing that happens in a
5 situation like that is the proprietors of systems who are
6 being assaulted, thusly, noted the address from which the
7 mail was coming and went to their routers or servers and
8 did some typing and suddenly those IPs were no longer to
9 deliver mail. And that was the first countermeasure that
10 you saw against that kind of event.

11 A somewhat more sophisticated set of Spammers
12 came along in late '95 and early '96 and became more
13 agile, you might say. One particular famous Spammer had
14 what he called a band width partners program where he
15 would basically freight you a server; you plug it in, you
16 turn it on, you're connected to your network and you ask
17 no questions and you accept his check. Thus when people
18 began adding his current IP addresses to their routers
19 and servers, he would simply fire up his next band width
20 partner and begin sending from that, until it, too, was
21 blocked.

22 That measure promoted another countermeasure,
23 largely -- essentially the ancestor of the blocking lists
24 that we see today. A man named Paul Vixie was rather
25 irritated at having to go and update lots of IP addresses

1 and various routers and various places, so he created a
2 realtime blackhole list, which became quite popular with
3 a number of system operators and whenever Paul would make
4 an update to his list as to where Sanford Wallace or one
5 of his other counterparts was sending from today,
6 suddenly that IP address would vanish all over the place
7 where anybody else who was accepting that feed was able
8 to block those essentially in real time, as soon as Paul
9 saw them coming in. Within half an hour, anybody who
10 subscribed to that list was also protected.

11 That was sort of the death nail for that
12 particular round of what I would call fixed-address
13 Spamming. And these were people on high-speed lines with
14 fixed IP addresses and the next obvious place to go was
15 someplace where there were just millions of possible IP
16 addresses you could send from, even if it was at low
17 speed, and that was the vast number of dial-ups that were
18 available. And at this particular time in history, I was
19 working for a dial-up ISP provider and got involved in
20 that particular series of events.

21 And what would happen in the most prolific
22 cases is a Spammer with a stack of prepaid, precharged
23 credit cards could sign up for, oh, two dozen, 300 or 400
24 different accounts at dial-up providers and use the dial-
25 ups, connect a machine to that and just send away at 28.8

1 or whatever speed he could obtain. And if you had enough
2 of these going at once, you might as well have a wide
3 band connection.

4 So, that particular method inspired its own set
5 of countermeasures. One of the first things that the
6 dial-up providers began to do was to configure their
7 systems so that when you're dialed in you cannot talk to
8 a mail server that's outside the network that you belong
9 to. You would be forced to send through your own server,
10 because at that time, the folks using the dial-ups would
11 use open relay servers, which you'll hear about shortly,
12 as their preferred method for both concealing their
13 origin and increasing their effective band width.

14 And, so, the dial-up ISPs began to do what is
15 called port 25 blocking, which prevents the user of a
16 dial-up account from communicating directly with an e-
17 mail server, other than the one that belongs to the
18 provider he's getting his connectivity through. And that
19 was for a while a real curb on the use of dial-up
20 accounts for Spamming.

21 However, it turns out for these
22 countermeasures, there are counter-countermeasures, some
23 very creative ones. One particularly prolific Spammer is
24 known to use a system in which a single machine has both
25 a broadband connection and a dial-up connection. And the

1 software inside has been hacked so that the packets to
2 the receiving server go out on the high-speed connection,
3 but inside the packet, the source address which says this
4 is where this packet came from, and if you're going to
5 reply to it, send it to this address. It happens to be
6 the address of the dial-up side. So, it will go out the
7 high-speed side and get replied to on the low-speed side.
8 And this gets around the port 25 blocking problem and the
9 fact that dial-ups aren't very fast.

10 There are various countermeasures to that that
11 I can't discuss.

12 **(Laughter).**

13 MR. RATHBUN: The other thing that will take up
14 a lot more of our time that Matt has already discussed
15 that solves the problem of port 25 blocking for dial-up
16 users is open proxies, because port 25 blocks port 25,
17 which is the SMTP connection; whereas open proxies use
18 any number of different possible input ports, and
19 depending on what kind of service the proxy provides, it
20 can end up coming out and talking to any number of
21 different kinds of services, whether it be telnet or HTTP
22 connections or SMTP connections or any number of other
23 things.

24 Now, as Matt mentioned, there are for some
25 providers the policy of going out and scanning the

1 customer's boxes to find out whether there's anything out
2 there that's vulnerable. I know that Roadrunner does
3 that; we do that as well. We don't have cable modem
4 subscribers, but we do have lots and lots and lots of
5 small businesses who may do any number of different
6 things to do connection sharing.

7 And we see -- as in the month of February, we
8 saw incidents of proxy abuse in our network. We received
9 about 1,300 complaints.

10 MR. FRANCOIS: I hate to interrupt you, but I
11 want you to hang on to those, because we're going to
12 return to them when we talk about open proxies in a
13 little further detail.

14 MR. RATHBUN: And the countermeasure to
15 scanning and customer education, the latest vogue is the
16 trojan proxy. We've begun to see these in our customer
17 networks, in which they get infected with a piece of
18 malicious software, which then installs a copy. In what
19 case, the sobig.a --

20 MR. FRANCOIS: Well, hang on. We're going to
21 talk about that, too. And things coming down the pike or
22 that have already come down the pike, so --

23 MR. RATHBUN: Let that thunder not be stolen.

24 MR. FRANCOIS: Exactly. But now we're going to
25 turn to Nick Nicholas, an internet consultant who is

1 going to talk to us about open relays.

2 MR. NICHOLAS: While I'm getting set up here,
3 I'd just like to thank the staff at the Federal Trade
4 Commission for inviting me to participate in this forum.
5 I also would like to commend the FTC for looking at this
6 very, very important issue, which as several other
7 speakers today have noted, costs in the billions of
8 dollars per year.

9 What I'm starting off here is just a few basic
10 schematics, showing how a relay works. The first
11 schematic shows the basic way an e-mail gets transmitted
12 from point A to point B. Literally we have a customer of
13 ISP A and they want to communicate with a customer over
14 on ISP B. Is my pointer even reaching over there? No, I
15 guess not. So much for my laser high-tech.

16 The mediating server is -- there's a server
17 that mediates between the ISP A and the ISP B, and the
18 customers of ISP B would actually communicate with their
19 own ISP's mail server in order to receive the e-mail
20 message. Now, it's possible, and Michael Rathbun has
21 already alluded to this, it's possible for a customer to
22 acquire software which will allow -- essentially turn --
23 instead of being at a normal workstation like this, you
24 can actually replicate the functions of a mail server.
25 And you can thereby bypass your ISP's mail server and

1 connect directly to the receiving ISP's mail server and
2 there reach any of the customers on that end of the
3 switch.

4 Now, this is the schematic that shows how an
5 unsecured mail relay works. We're still a server here,
6 and rather than connect directly, the reasons Michael has
7 mentioned some of the reasons you might not want to do a
8 direct connection, traceability is the main point. Find
9 an unsecured mail server. These are rather easily found.
10 There are Spammers out there who will sell you lists of
11 unsecured mail servers. I think they go for about a
12 dollar each. And if you want an anonymizing server,
13 which will actually disguise the actual source of the
14 mail, those go for about \$2 a pop. So, the mail will
15 actually go through the unsecured mail server and then
16 onto the receiving ISP's mail server and thereon to all
17 the fortunate recipients behind ISP B.

18 The final schematic I wanted to show actually
19 combines the two tactics we've discussed so far. We've
20 got ISP C down here now, and this little red machine here
21 is an open proxy, and it is possible to chain an open
22 proxy with an unsecured mail server and thereby disguise
23 the actual source of the message. It will look like the
24 message is actually originating from here, and in that
25 way you'll get complete anonymity in what the actual

1 sources in the mail messages are.

2 Now, I was going to give a brief -- an actual
3 how-to. Are there any Spammers in the audience? No real
4 mail servers were used in this demonstration; no laws
5 were broken; and most of all, do not try this at home. I
6 picked up from a recent spam that I received a -- it was
7 sent through an open relay, kension.plus.com, and you
8 begin this process. Margot sort of stole my thunder by
9 doing this same demonstration. You simply use a
10 convenient utility called telnet, which allows you to
11 remotely access machines, and that colon-25 on the end is
12 important, because that's where the simple mail transport
13 protocol is listening.

14 And it will respond with the message saying --
15 identifying itself, letting you know that it's ready to
16 go. It will also tell you what mail transport agent is
17 being used. And, so, I now say hello, misspelled helo.
18 Now, I'm using some of the Spammer tricks in here, so
19 this is actually overlapping a little bit with some of
20 what was covered in the previous panel. Helo
21 hotmail.com. Now, of course I'm not hotmail.com, but I
22 want the receiving mail server to think that I am. And
23 it will simply respond okay. It will accept whatever I
24 tell it it is.

25 Then I tell it that I'm sending mail from

1 president@whitehouse.gov, and it will tell me that sender
2 is okay, even though, of course, I'm not
3 president@whitehouse.gov, at least not yet. Then you
4 identify the recipient, this is all specified in the
5 protocols, rcpttodrumsfeld@dod.gov, and it will say that
6 that recipient is okay as well. Now, I enter data, and
7 it will tell me it's ready for -- ready for me to go.

8 The first thing I'm going to do as a Spammer is
9 put in some forged header information. I want the
10 headers to reflect the fact that this really did come
11 from hotmail, and I even did a little bit of homework. I
12 found out that one of the IP addresses for
13 mail.hotmail.com is in fact 65.54.254.129. And, so, I
14 very carefully constructed this header, this particular
15 data point, so that the recipients are going to be fooled
16 by this, more than likely than not. This is still data -
17 - what we put in the mail from doesn't necessarily have
18 to reflect what's said here, but I am for convenience
19 sake. To drumsfeld, subject, invasion of France.

20 **(Laughter).**

21 MR. NICHOLAS: Please proceed immediately with
22 plan for invasion of France, G.W. Bush. And here's that
23 tiny little period there that lets you know I'm done with
24 the data part.

25 MR. FRANCOIS: You're going to get me in

1 trouble with the international panelists, and the
2 international division.

3 (Laughter).

4 MR. NICHOLAS: I picked this for you.

5 MR. FRANCOIS: It's been a great job while I've
6 had it.

7 (Laughter).

8 MR. NICHOLAS: And the period is important.

9 The period tells you that you've concluded with the data
10 section, and it's set. It says mail is queued for
11 delivery. At this point I could identify new recipients,
12 but instead I'm just going to quit and it signs off,
13 closing connection, good bye. And it's really -- it's
14 that easy. And that's why hundreds of Spammers, if not
15 thousands, do it daily.

16 Just before closing out, I wanted to talk a
17 little bit about the scope of the problem. It's actually
18 an old problem. It's been a problem at least since 1996,
19 but it is still a problem. The MAPS RSS has a little
20 under 180,000 open relays listed. Another list run by
21 Osirus Soft has over 190,000 listed. The open relay data
22 base has 182,000 listed. DSBL has 214,000; and the
23 NJABL, not just another bogus list, has 255,000 listed.
24 There is some overlap between the lists, but not
25 completely so.

1 Most of the experts think that we have at best
2 half of the open relays identified. So that means that
3 there are approximately half a million open relays out
4 there that can be abused. The problem is not going away.
5 I know of some ISPs that check incoming connections to
6 see whether or not the mail server that's trying to make
7 a connection is an open relay. I've heard from one ISP
8 that they're finding 400 new open relays a day.

9 Mark, if I can put you on the spot for just a
10 second, I know that Roadrunner does this, can you give me
11 an estimate of how many open relays you're finding? Is
12 400 a conservative estimate?

13 MARK: Based upon the amount of mail we get,
14 it's a conservative estimate.

15 MR. NICHOLAS: Four hundred is conservative.

16 MR. FRANCOIS: Mark in the audience said that
17 400,000?

18 MR. NICHOLAS: Four hundred new ones.

19 MR. FRANCOIS: Four hundred new ones is a
20 conservative estimate.

21 MR. NICHOLAS: Every day.

22 MR. FRANCOIS: I just wanted to repeat that for
23 the people listening.

24 AUDIENCE MEMBER: (Inaudible) -- we have more
25 than that.

1 MR. NICHOLAS: You find more than 400 a day?

2 MR. FRANCOIS: What we're going to -- I'm sorry
3 to cut you off, Nick, but we want to kind of save the
4 questions and comments from the peanut gallery, so to
5 speak.

6 MR. NICHOLAS: Okay, I just wanted to get some
7 real world input. So, 400 is -- 400 new ones a day is a
8 conservative estimate.

9 MR. FRANCOIS: Right.

10 MR. NICHOLAS: So, it is an old problem, as I
11 say, but it's still a problem that's with us today.

12 MR. FRANCOIS: And I'm going to go ahead and
13 kind of open up questions to the panelists about open
14 relays and open proxies. We just heard that 400 new open
15 relays a day -- does anybody have any information in
16 terms of how much are getting put on blocklists a day or
17 a week?

18 And if you could go ahead and identify
19 yourself.

20 MR. NICHOLAS: Nick Nicholas again. Each of
21 the relays are different; each of the lists are
22 different. But it ranges from anywhere from as few as 50
23 a day to a couple hundred a day. And these blocking
24 lists, though, are very effective in getting rid of --
25 getting some of these open relays closed. So, there's

1 quite a bit of turn in the number of relays that are
2 open. So, they are getting closed, but as soon as some
3 get closed, there are others being uncovered.

4 MR. FRANCOIS: Close anywhere from 50 to 200 a
5 day, but --

6 MR. NICHOLAS: Correct.

7 MR. FRANCOIS: -- you're still getting at least
8 400 a day opened?

9 MR. NICHOLAS: Right. So, the problem is
10 growing rather than shrinking.

11 MR. FRANCOIS: Is there any way -- oh, go
12 ahead, I'm sorry, Matt.

13 MR. SERGEANT: For open proxies, the figure is
14 about -- on average of about 2,000 a day, coming on-line.

15 MR. FRANCOIS: Two thousand being discovered?

16 MR. SERGEANT: New ones being detected.

17 MR. FRANCOIS: Detected? And likewise, the
18 same question, how many are being put on blocklists a day
19 in your estimate?

20 MR. SERGEANT: That data is based on
21 blocklists.

22 MR. FRANCOIS: Okay. So, 2,000 coming up
23 active and then afterwards, when they're discovered, how
24 many get put on the list and deactivated, or can they be
25 deactivated?

1 MR. SERGEANT: There is some evidence of slight
2 decreases, but nothing nearly dramatic enough.

3 MR. FRANCOIS: Okay. In terms of open relays,
4 I know that -- is it possible -- you gave a demonstration
5 where there were forged headers, and one of my questions
6 was whether that was done automatically or by hand, and
7 if it's done by hand, by a particularly diligent Spammer,
8 is there any way for a person who has received mail to
9 track it through an open relay and to the originating
10 source?

11 MR. NICHOLAS: I just did that by hand as a
12 demonstration. There's actually software that automates
13 that entire process and is able to do hundreds of
14 thousands of these per hour, so it would be quite tedious
15 to try to do a couple hundred thousand per hour by hand.

16 What was the second part of your question?

17 MR. FRANCOIS: The second part of the question
18 was basically addressing --

19 MR. NICHOLAS: Oh, if you can -- you can't tell
20 from the headers themselves whether it came from an open
21 relay or an unsecured proxy. The headers themselves
22 won't reveal that information. You'd actually have to
23 scan the machine to see what ports were open. A good way
24 to do that, without necessarily scanning the machines
25 yourselves, is to check some of the lists -- I listed

1 five there -- and see if it's already been determined to
2 be an open proxy or an open relay.

3 MR. FRANCOIS: Okay, but even if you send spam
4 through an open relay and I trace it through the header,
5 it won't eventually come back to you?

6 MR. NICHOLAS: Not necessarily. Not
7 necessarily. There are anonymizing relays and especially
8 if you do a chain process where you combine an open proxy
9 with an unsecured relay, the chain will actually stop at
10 the open proxy, and it will look as if the open proxy is
11 the source of the message.

12 MR. FRANCOIS: A quick question about the
13 number of potential ports that a proxy or an open proxy
14 can be -- that can be exploited by an open proxy. Just a
15 rough estimate of how many ports are out there and how
16 many ports are available that can be exploited?

17 MR. SERGEANT: Well, theoretically, the total
18 number of ports is about 65,000, but generally they tend
19 to fall into specific ports for specific pieces of
20 software, so you can actually go out and look
21 specifically for port 8080, or port 1080, or something
22 like that, for a specific type of proxy server. But more
23 and more we're seeing open proxies appearing on
24 randomized ports, which obviously is a much more
25 difficult problem to deal with. That tends to be -- that

1 tends to fall into the area of trojans.

2 MR. FRANCOIS: I know that there's been a lot
3 of numbers bandied about today, and probably for the rest
4 of the forum, in terms of the amount of spam sent per day
5 in relationship -- or the amount of e-mail sent per day.
6 Is there any way or do you all have any evidence that
7 indicates how much spam on a daily basis is sent through
8 open relays and through open proxies, or as a matter of a
9 percentage?

10 MR. PATTON: I would say through my own
11 experience -- this is Brad Patton -- that recently,
12 especially within the last few months, 40 to 50 percent
13 of all the spam relayed to our network or through our
14 network is done so using open proxies or open relays.

15 MR. FRANCOIS: Okay. Michael?

16 MR. RATHBUN: During the month of April, up
17 until the 26th, looking at the just raw count of unique
18 IP addresses involved in a spam sample of 4,571 addresses
19 that had been tested during the month, 55.1 percent were
20 already identified as open proxies on one or both of two
21 different lists that were in use. So, the number's
22 higher than that --

23 MR. NICHOLAS: I've actually heard numbers as
24 high as 95 percent are being sent through unsecured
25 proxies. Proxies seem to have overtaken relays in terms

1 of what kinds of systems are going to be abused.

2 MR. FRANCOIS: How recently has that --

3 MR. NICHOLAS: I would say this was within the
4 last few months that they jumped to a number that's that
5 high. Now, these are smaller systems that ISP
6 administrators are reporting that as many as 95 percent
7 of the spams they're receiving have already been listed
8 on one of the open proxy lists.

9 MR. FRANCOIS: Okay. In terms of mail servers
10 and open relays, are relays left open intentionally for
11 spamming, unintentionally? Why does that --

12 MR. NICHOLAS: Well, that's a good question,
13 actually. There are -- particularly in corporate
14 environments, some corporations will leave their mail
15 servers unsecured so that executives and sales folks who
16 are on the road will be able to still use those mail
17 servers, regardless of where they're dialing in from.
18 Typically, you may be dialing in a dial-up at a hotel.
19 And, so, they'll leave the home server, so to speak, open
20 so that they sales folks or the executives won't have to
21 make any changes in the configurations on their mail
22 clients.

23 So, it's done largely as a matter of ease of
24 use for certain corporate end-users. So, it does have a
25 valid use. There are ways around that, though. that's

1 not necessarily the only way you can accomplish that end,
2 but it's the simplest way, and some people want to go for
3 the simplest solution possible.

4 MR. FRANCOIS: Is it also that the tools for
5 authenticating users and access to the network have
6 gotten so much better over time that there's really no
7 need to leave a relay open?

8 MR. NICHOLAS: I would agree with that
9 definitely.

10 MR. SERGEANT: Absolutely 100 percent. There
11 is no technical reason now that you need an open relay.

12 MR. FRANCOIS: Can anybody proffer a reasonable
13 reason for maintaining an open relay?

14 UNIDENTIFIED SPEAKER: I can't think of one in
15 today's context, honestly, no.

16 MR. FRANCOIS: What about open proxies in terms
17 of -- I know that there -- proxies serve a valid
18 function, caching remote access and you've spoken a lot
19 about the insecurities in them. Are the insecurities --
20 again, are they intentional? Are they unintentional? Is
21 it a mistake of the user confusing -- trying to set up a
22 web server and they make a mistake? Is it being shipped
23 in the box that way?

24 MR. SERGEANT: I would say that 99.9 percent of
25 the time it's unintentional. It seems that --

1 MR. FRANCOIS: And unintentional -- I'm sorry
2 to cut you off -- and unintentional on whose part as
3 well.

4 MR. SERGEANT: From the person who installed
5 the proxy server. It's unintentional that it was set up
6 insecurely. I'm sure if you were able to contact the
7 people who were running them, they would probably be
8 quite surprised and confused. Most of the software that
9 does this seems to be set up by default to be insecure,
10 and that's one of the biggest problems.

11 A number of people have actually spoken to the
12 authors of these software packages to try and instigate
13 some change there. And some of them have fixed the
14 problems; and some of them are disinterested.

15 I'm sorry, there was another part of your
16 question, as well.

17 MR. FRANCOIS: Yes, we just combined the parts,
18 so you answered both of them. One other question about
19 open proxies and open relays. What is -- I guess all the
20 people that contact individuals that are operating open
21 proxies and open relays, what has been generally their
22 response? Is it shock, amazement and cooperation or
23 indifference?

24 MR. PATTON: I would say through my experience
25 it would be bewilderment and they don't really believe

1 that so much mail has been sent from their network or
2 through their network, but it's usually, once you get the
3 person calmed down, or explain exactly what's going on,
4 it's usually a simple fix. It's just a misconfiguration
5 of the actual software, and if you can explain it to
6 them, normally it takes about 10, 15 minutes to resolve
7 the issue.

8 MR. FRANCOIS: Adam?

9 MR. BROWER: I'd like to interject. My name is
10 Adam Brower, by the way, I'm a citizen of the United
11 States. I'd like to interject kind of a sociological
12 note, and that's really why I'm here. I don't pretend to
13 have the technical expertise of some of the other
14 participants, but I've had some experience dealing with
15 administrators in other cultures, and in particular in
16 Asia I found that the concept that an unsolicited
17 approach to business -- it's hard to make the point
18 initially that it's unwelcome, because in Mayan cultures,
19 it's honored, it's considered a very polite thing to do,
20 and it's an honor to be so requested and so solicited.

21 And I must say that kind of goes along with
22 what Brad was talking about, amazement, that bewilderment
23 is not only technical and not only evidenced by, you
24 know, raised eyebrows and I can't believe this is
25 happening, but also I can't believe it's a problem. And,

1 so, you know, a lot of times there's a technical issue in
2 terms of the language in which documentation is often
3 written, which is usually English; and there's another
4 problem, a cultural problem, in making clear to some
5 administrators that it really is an issue, at least in
6 our culture, in our society.

7 MR. FRANCOIS: And that brings us to a good
8 juncture to kind of talk about international aspects of
9 open relays and open proxies, in terms of how much spam
10 is sent through relays that have IP addresses of other
11 countries.

12 MR. BROWER: In my experience, I mean, I don't
13 want to tar any particular nation with the spam brush,
14 but it's a moving target, as I'm sure others can attest.
15 Brazil has come to the fore recently. And an interesting
16 anecdote, recently in conversations with a Brazilian
17 administrator, he found it annoying that the
18 international language of the internet, by no one's
19 design, I think, has become English. And he said to me,
20 well, why can't we converse in Portuguese, and I had to
21 say, well, because your English is noticeably better than
22 my Portuguese. And then I said also, I mean, I'm not
23 sure about this, but I imagine if you tried to land a
24 plane in Sao Paulo and speak to the tower in Portuguese,
25 you'll be turned back. That's just an unfortunate fact

1 of life, but it's one that can be remedied.

2 And I think one thing that we can address, and
3 again, this is a nontechnical issue but a social
4 engineering issue, one thing I think that everyone could
5 address is to find methods to get documentation,
6 including easy fixes, including deep documentation,
7 available in many, many more languages than they are
8 currently available in. That in itself would solve a lot
9 of the problem, I think.

10 MR. FRANCOIS: I know that previously we had
11 spoken about spam that you had received that had been
12 sent through a relay in China.

13 MR. BROWER: Mm-hmm.

14 MR. FRANCOIS: And while you know a little bit
15 of Mandarin.

16 MR. BROWER: Very, very little.

17 MR. FRANCOIS: I want to get you to discuss
18 some of your experiences with trying to communicate.

19 MR. BROWER: Oh, well, I mean, I just -- I
20 actually just -- again, I don't want to name names in a
21 public forum, but, I mean, I will tell you that one
22 particularly -- one point I made before, and I'll make it
23 again. I again and again encountered administrators who
24 said to me that it's an honor to be solicited for
25 business. And I want to stress this as a socio-cultural

1 issue. It's not strictly and only a technical issue. I
2 think we err when we approach it strictly as technical.
3 In other words, is this proxy exploited, how do we get it
4 closed? We need first to understand that the way in
5 which we perceive the internet is not necessarily the way
6 in which the rest of the world perceives it.

7 And, you know, I can -- are you referring to
8 one particular -- you want to refresh my memory? Was
9 there a particular anecdote we discussed, Renard?

10 MR. FRANCOIS: No, no, it was just something
11 that I had scribbled down in my notes.

12 MR. BROWER: I wish you'd share it with me.

13 MR. FRANCOIS: Just talking about how difficult
14 it was in terms of, first of all, the two barriers that
15 you'd enumerated, the first was the barrier, the language
16 barrier.

17 MR. BROWER: Mm-hmm.

18 MR. FRANCOIS: And trying to --

19 MR. BROWER: The socio-cultural one.

20 MR. FRANCOIS: Right. And then the second
21 barrier being the socio-cultural area.

22 MR. BROWER: I can tell you this, that even --
23 I mean, interestingly enough, a couple of times I had in
24 dealing with networks in China, I had to battle through
25 to find the -- you know, the person whose English was

1 sufficiently superior to my Chinese that we could carry
2 on in a rational conversation. And even at that point,
3 many times I encountered that same cultural barrier,
4 amazement that it was considered -- and by the way, we're
5 talking -- also I should put it in context. This is a
6 year and a half ago. There's obviously been significant
7 education since then among many Chinese admins, due not
8 in small part to the efforts of people like Steve Linford
9 (phonetic) and Chinese admins all name Ed Yu (phonetic)
10 as a good example of someone who's made a personal effort
11 to educate administrators in mainland China. But, you
12 know, some of the reactions I got were actually funny,
13 but I don't want to really tar anyone.

14 MR. SERGEANT: Well, actually I can expand on
15 that, as well.

16 MR. FRANCOIS: Excuse me, Matt?

17 MR. SERGEANT: I can expand on that, as well.
18 That we've definitely seen a shift where we have kind of
19 a unique perspective, being a global company, that we're
20 seeing more and more customers in places like Korea
21 coming to us and saying that actually we didn't believe
22 spam was a problem but now it really is an issue, and we
23 would like to stop it. So, there is some movement going
24 on in those Asian nations to change their outlook.

25 MR. FRANCOIS: Go ahead, Dr. Hancock.

1 DR. HANCOCK: One of the things, we operate in
2 82 countries, and so we deal with this on a multi-
3 national basis on a regular basis. I was at a forum in
4 Japan just about a month ago, and one of the discussions
5 there was how to cut down spam, and if it wasn't for the
6 classic reason of spam is objectionable, it was because
7 it was sucking up bandwidth. And as a result of that,
8 that communication got through to the Japanese customers
9 quite quickly, because someone is illegally using your
10 bandwidth and illegally using your computers and taking
11 away your resource, irrelevant of what it was. And that
12 got their attention rather quickly.

13 When you tried a discussion with them on a
14 social basis in terms of it's a security violation, it is
15 objectionable content and all that, you have to remember
16 that in other countries, such as Japan, child pornography
17 is legal.

18 And, so, when you start dealing with different
19 kinds of aspects of spam and what the content of the spam
20 might be, in that country it might be a legal thing. But
21 when you start addressing it as a someone's using your
22 bandwidth, all of a sudden it became a very serious
23 problem and the conversation changed quite radically.
24 And, so, what you'll find is that I agree with the
25 sociological issues, but I think one of the things you do

1 is you approach it as band width theft in those areas or
2 space theft, and all of a sudden it becomes a very
3 serious ordeal when you start dealing with folks in the
4 other countries.

5 MR. FRANCOIS: And, Adam, I wanted to kind of -
6 - and maybe this is a question for all of you who have
7 dealt with the problem of international open relays, is
8 to ask once you get past the first and the second
9 obstacles, the language barrier and the social barrier,
10 do you find that the system admins are particularly
11 helpful and willing to resolve the issue?

12 MR. BROWER: I would say anxious to. You know,
13 once they're apprised of the actual problem, but again,
14 there still is the barrier of language in the
15 documentation, and I think that's a serious shortcoming
16 and one that we have not addressed as, for want of a
17 better phrase, as a community. I'm not sure we are one,
18 but as a nascent community, I think that's something we
19 could address. Making, you know, world lingo and
20 babblefish and other on-line translation services are
21 notoriously hilarious in their renderings of technical
22 language particularly.

23 And, so, you know, I think in line with what
24 Bill said, making the point that theft is frowned upon in
25 every society, I guess is a good way to boil that down.

1 And then having documentation that makes it very clear to
2 admins how to fix security holes in their software in
3 their own language will facilitate that. So, I really
4 think that the availability of documentation in various
5 languages is a very important issue and needs to be
6 addressed.

7 MR. FRANCOIS: There are two follow-up
8 questions that I wanted to ask about international open
9 relays and proxies. The first would be out of the
10 400,000 -- or approximately 400,000 open relays that Nick
11 told us about, is there any way to quantify how many of
12 those are international?

13 MR. NICHOLAS: My guess is it's the majority of
14 them are. And that's just derived from my experience in
15 studying the issue over the years. I can't quantify it
16 any further than that. But they particularly seem to be
17 in the lesser developed countries, where the level of
18 education is not quite as great as it is; the sensitivity
19 to the issues is not quite as great as it is in the
20 States. But certainly the United States is not immune
21 either.

22 MR. FRANCOIS: And also in terms of open
23 proxies, is there any way -- is that an international
24 problem, as well, or is it mostly domestic? Michael?

25 MR. RATHBUN: Well, the problem is being dealt

1 with, but there was a time when the standard issue system
2 that was put into Korean public schools was a software
3 load that included an open mail server and an open proxy.
4 And that was a bonanza, to the point where there was, in
5 fact, a DNS-based advisory list that would specifically
6 tell you, yes, this IP is in Korea. And, again, this is
7 something that the Koreans themselves have been grappling
8 with, and I know we'll hear more about this later on in
9 the forum.

10 But it highlights a particular kind of genesis
11 of this problem from my perspective, which we touched on
12 to some degree earlier, in that in many cases what we
13 have is something that was built to be insecure, either
14 because in the case of some of these software loads they
15 were put together when open proxies and open relays were
16 not customarily abused or there is just resistance to
17 what I would call a product quality and a safety and
18 suitability issue.

19 MR. FRANCOIS: Actually, I lied, I still have
20 two more follow-up questions on this. The first is we'd
21 heard on a previous panel that a panelist said that
22 Spammers were paying open relay or operator systems
23 administrators to maintain open relays internationally.
24 And I'm just wondering, is that your experience? Is
25 there anecdotal evidence that you found about that, that

1 people are actually in the United States giving money to
2 people internationally to keep an open relay?

3 MR. BROWER: I can speak to that anecdotally,
4 and again, without naming names, I should say that it's
5 part of my practice as an independent consultant I often
6 have to deal with what in military terms would be termed
7 dark sources. But I had occasion once to speak to an
8 administrator in Romania and was told shortly before he
9 cut the wire that he had been given a certain honorarium,
10 and again, I hate to use the name -- the word certain, by
11 a certain American, relatively well known entrepreneur,
12 let's just say. And when I informed him that I was going
13 to forthwith deny those IP addresses to the deny tables
14 to which I had access and that I would recommend others
15 do the same, he I guess had further negotiations with the
16 American entrepreneur and sacrificed the remainder of his
17 honorarium. So, yes, in short, I have personal anecdotal
18 evidence that it is possible to bribe someone to keep a
19 relay open, sure.

20 MR. FRANCOIS: Dr. Hancock, you look like you
21 were shaking your head down there.

22 DR. HANCOCK: Well, I've seen both extremes,
23 but to be frank about it, the bulk of the folks that we
24 run into, because we have embarked on scanning our
25 network, and you're talking about 3 million IP addresses

1 just in Asia alone. When we contact the customers, by
2 and large in Asia and in Europe, the customers are
3 shocked that they are able to be used. We have run into
4 very, very few that are actually being paid to keep the
5 relays open or to keep a proxy open.

6 Now, the bulk of the situation that we've run
7 into with proxies is that a lot of proxies that were
8 originally developed were part of like firewall tool kit
9 and things like that, and those proxies out there were
10 for generic purposes so that you could use other
11 protocols through it, as well. As a result, those
12 technologies are still there, and they are used for other
13 protocols like Tuxedo and what have you like that, and
14 they make a very nice place to go back and relay e-mail
15 through, as well.

16 So, what you find out very quickly is that a
17 lot of people have these things open because they were
18 there all along or they need it for another protocol.
19 But what you'll find also is that they don't necessarily
20 keep them open because they're being paid for it. Now, I
21 don't disagree that there are some cases where that is
22 the case, but by and large what we've run into with our
23 customers is they're usually shocked that they're
24 involved in something like that and they didn't know that
25 it was open to start with, or they had it open for a

1 specific reason that had nothing to do with e-mail.

2 MR. BROWER: Yeah, I certainly didn't mean to
3 imply that it was an endemic problem, but only that in
4 fact it does happen.

5 MR. FRANCOIS: And the final question, before
6 we kind of close out this issue, is just a question from
7 my perspective is it is easy to tell, and if it is, how
8 much spam is actually generated in this country but
9 relayed internationally back to this country?

10 MR. NICHOLAS: Yes, it is easy to tell. That
11 much you can generate help from headers, and there is
12 quite a bit of that going on. What appears to be
13 international spam originating from Chinese servers
14 actually originated in the United States. We know this
15 because the spam itself is in English. They are
16 promoting American-based companies and American-based
17 websites.

18 MR. FRANCOIS: Anyone else?

19 Okay, so moving on to -- Matt and Nick briefly
20 talked about kind of resolving the situation with relays
21 and proxies and talked about patching or reconfiguring
22 their systems. And my general question is for open
23 relays -- for both relays and proxies how easy or
24 difficult is it to reconfigure the system for the
25 intended user or the person that is most likely to be the

1 one that has installed the relay or proxy, whether it's a
2 systems administrator or a person at home trying to
3 create their own network? And also in addition to how
4 easy it may or may not be, is it very expensive to do?

5 MR. NICHOLAS: I can speak on it to the proxies
6 issue, and I'll let -- I'm sorry, relay issue; I'll let
7 Matt deal with the proxy issue. It's actually very
8 simple in most cases to lock down a server that is
9 unsecure. Often it's just a matter of a single
10 configuration line in a configuration file. The problem
11 is knowing which line it is that needs to be locked down,
12 so there is some amount of education that's required in
13 order to do this, but I would say by and large the time
14 and effort is relatively minimal.

15 MR. FRANCOIS: Now, in terms of the education,
16 do they find that on a website? Do they get a
17 contractor?

18 MR. NICHOLAS: MAPS sponsors something called
19 the transport security initiative, and the whole purpose
20 of this project was to make the information needed to
21 secure various programs, whether it be sendmail, queue-
22 mail, post-fits, et cetera, it would tell you exactly
23 what you needed to do to go in and lock down that server.

24 MR. FRANCOIS: Okay. Matt?

25 MR. SERGEANT: As far as open proxies go, it

1 changes slightly more, because there seem to be more
2 pieces of software for running open proxies than there
3 are for running SMTP servers. But in general, the most
4 common piece of software we seem to see is Analog X, and
5 changing its configuration is a matter of opening the
6 preferences dialog, entering an IP address, clicking OK
7 and then it's done.

8 MR. FRANCOIS: Anybody else? How big -- in
9 terms of the amount of spam that we are probably going to
10 discuss on Thursday and Friday being problematic and the
11 enormous costs that imposes on businesses, ISPs and
12 consumers? And I know it's speculation, but how much of
13 that do you think is attributable to spam sent through
14 open relays and open proxies?

15 MR. RATHBUN: Again, what I've noticed on
16 Earthlink's network is that 40 to 50 percent of the spam
17 sent to our network or really through our network is due
18 to misconfigured proxy servers or open relays, at least.

19 MR. FRANCOIS: And of the 40 percent of the
20 spam that you all get through open relays or proxies, as
21 a percentage, how much do you think that you all are able
22 to find, process and take action upon, whether it's
23 contacting the relay operator or server owner and taking
24 -- advising them to take steps to close the relay or
25 secure the proxy?

1 MR. RATHBUN: With mail sent to our network
2 that did not come or was not relayed through it, we will
3 send off reports to the originating networks or the
4 networks where the mail was relayed through, so I can't
5 speak to how many of those issues get resolved, but for
6 our own -- on our own network, a good portion of my day
7 is spent calling customers with these problems and making
8 sure that they all get secured.

9 I'd say if -- out of the percentage of mail
10 that was sent from our network through using these
11 insecurities, close to 100 percent of them, as long as
12 they get reported to us, get resolved; or we will resolve
13 them on our own.

14 MR. FRANCOIS: And how will you do that?

15 MR. RATHBUN: We may have to shut down service
16 for a time, but normally that's when we'll get a quick
17 call from the customer.

18 MR. FRANCOIS: So, we've talked about kind of
19 the open relays, proxies problem; talked about a cost-
20 effective way to try and remedy those situations, and I'm
21 going to turn to Brad to talk about another potential
22 solution that you can use for probably a couple of ways,
23 and that's honeypots and what they are and what they do
24 and what you do with them.

25 MR. PATTON: Honeypots are computers that are

1 connected to the internet and are designed to look like
2 an ordinary or insecure, in this case, mail server or
3 open proxy. They can be used as a tool to detect illicit
4 activity on that computer. From that information, we can
5 detect trends or specific problem IPs where we are
6 getting scans to the honeypot, scanning for an open relay
7 or an open proxy server. So, it can be a useful tool if
8 used correctly.

9 MR. FRANCOIS: What types of information do you
10 all -- does the honeypot get from people who are trying
11 to manipulate the system?

12 MR. PATTON: It would show you who was logged
13 in and from where, if you could find out where that IP
14 was located. Basically you can detect trends to see if a
15 lot of people are scanning for a certain type of
16 insecurity or if it's coming from a certain region, and
17 perhaps you can take measures to filter some of the
18 traffic coming to your network from that area.

19 MR. FRANCOIS: What region do you find mostly
20 is trying to get into the Earthlink system?

21 MR. PATTON: I wouldn't know any specific
22 region where they were coming from.

23 MR. FRANCOIS: Okay. The other thing that --
24 have you all used from the information, and you may not
25 know about this, and other panelists may, but have you

1 used information that you've gathered in using honeypots
2 to litigate against Spammers?

3 MR. PATTON: Not to my knowledge.

4 MR. FRANCOIS: Okay. And do you know roughly
5 how much on a daily basis maybe you acquire the
6 information, process it and maybe block a particular IP
7 address based on what you find in those?

8 MR. PATTON: I wouldn't know any specifics with
9 that. We use what you would call spam-trap addresses
10 more than honeypots. A spam-trap address is what a
11 honeypot is to a server, a spam-trap address is to all e-
12 mail addresses. It's an address that is basically a
13 dummy account where no one signs up for any e-mail lists,
14 no spam or anything like that, and after a time, spam
15 will be sent to that address, and you know that anything
16 sent to that address, because it's never been signed up
17 for any list, is obviously unsolicited e-mail. And,
18 again, you could use it the same way as you would a
19 honeypot, try and see where this mail is coming from, if
20 you can block the sender from sending more mail to your
21 network, because again, you know it's spam right away if
22 anything gets sent there.

23 MR. BROWER: Could I interject something here?

24 MR. FRANCOIS: Yeah, sure.

25 MR. BROWER: I heard a tale of a woman named

1 Nadine.

2 (Laughter).

3 MR. BROWER: I wonder how many of you are
4 acquainted with Nadine.

5 MR. FRANCOIS: If you can do it briefly, you
6 might want to go ahead and explain.

7 MR. BROWER: Well, I think I may defer to Mike
8 on this.

9 MR. RATHBUN: I'll tell you that Nadine is
10 getting an increasing number of pieces of e-mail every
11 day that are relayed through open relays and open
12 proxies, and the last time I did an analysis of the
13 Nadine traffic, in fact, the trend was toward an open
14 proxy feeding an open relay.

15 For those who don't know, I operate a small
16 domain that at one time accepted mail addressed to
17 anything, and a woman in the southern United States
18 signed up for a sweepstakes one day and gave an address
19 that was on my domain. I had never met the lady and
20 haven't yet, but since that time in the year 2000, her
21 address has propagated all over the place and fallen into
22 the hands of the most amazing variety of mailers.

23 Given that she actually failed to exist, it
24 could be argued that she failed to opt in to any of these
25 things. So, Nadine is kind of a special case spam-trap

1 address, because it was basically an address that was
2 acquired by a major mainstream reasonably legitimate
3 mailer with the belief on their part that it was actually
4 given to them with the permission of the actual account
5 owner. It wasn't, so that's really pointing out part of
6 the security issue. But it escaped from the realm of
7 more or less legitimate respectable mailers out into what
8 I call the world of the gutter Spammer approximately nine
9 months. And now it's quite a menagerie.

10 MR. BROWER: Mike, what's the current volume of
11 Nadine's accumulated message load? Do you have an
12 estimate?

13 MR. RATHBUN: Well, it's difficult to say,
14 because as things stand now, I let any given mailer have
15 three shots, and then I block them.

16 MR. BROWER: You would have run out of disk
17 space theoretically by now --

18 MR. RATHBUN: Right.

19 MR. FRANCOIS: One thing I want to turn to you,
20 we've talked about proxies, relays and honeypots and
21 potential solutions. I want to talk to -- and we've
22 heard Michael Rathbun eloquently describe the escalation
23 that goes on or that has gone on from a dial-up account
24 to the ISP response to the Spammer response to that by
25 going to relays, the response to that by -- and then the

1 Spammer responds by going to open proxies and it just
2 seems like for every action there is a reaction from the
3 Spammers. And, so, part of -- the last part of this
4 panel is going to talk about the future of spam and the
5 exploitation of security weaknesses that have started.
6 And we're going to turn to some issues that have come up
7 in the last six weeks and I'm going to start off with
8 Adam Brower on that, and we will then talk about -- and
9 then we will move to a closing presentation from Dr. Bill
10 Hancock. And, so, we've got about 11 minutes.

11 MR. BROWER: Okay, I'm going to try and talk
12 very fast. No, no, I'm only -- I'll talk slowly.

13 MR. FRANCOIS: Well, we're going to save time
14 for some questions, so that's more.

15 MR. BROWER: I'll still try to talk fast or
16 quickly and properly. I wanted to raise an issue that
17 was raised at the first panel today, and that is the
18 issue of zombie or legacy blocks, which seems to be the
19 flavor of the month. And I've been involved in a couple
20 of interesting BGP shenanigans recently, trying to chase
21 down the perpetrators of them. Briefly, for those of you
22 who don't, you know, aren't up on this or aren't aware of
23 it, I can -- being myself a layman, I can probably
24 describe some of it in layman's terms.

25 A company, Xco, has a domain, xco.com, and they

1 wind up getting a block of IP addresses. And in the
2 fullness of time, xco.com goes out of business. And for
3 whatever reason, be it good bookkeeping or just anxious
4 to get down to the Bahamas and play with their boats,
5 they don't -- there's no traffic issuing from that block
6 of IP addresses. It's just sitting there; it's not used;
7 it's not announced anywhere even. And by announced I
8 mean it's not propagated to all the other computers; it's
9 not visible to the internet at large.

10 So, along comes an enterprising -- again I have
11 to use the term entrepreneur, who says to himself, well,
12 how hard would it be for me to make a piece of
13 letterhead, representing myself as xco.com. People at
14 ARIN may not be aware that xco.com is out of business.
15 And lo and behold, that works. What happens is that
16 zco.com winds up controlling xco.com, and then they
17 contact the backbone and say we're in control of this
18 block and we would like you to announce it. And lo and
19 behold, backbone X announces it.

20 This is very much social engineering, in the
21 classic sense of the term. And a lot of it's done by
22 telephone and fax. I really am Bill Jones of xco.com,
23 and honestly, you know, we just want you to announce this
24 block for us. I've seen it happen, and inevitably, of
25 course, or maybe it's obviously inevitably what the

1 material that the websites wind up hosting those IPs is
2 bogus in every sense of the word.

3 Now, as it works out now, there's kind of an
4 unofficial -- I won't say cabal -- I'll say group of
5 people who gather in various media to discuss these
6 issues, typically in tones of outrage, how could it be
7 that so-and-so is announcing such-and-such a block? And
8 then what generally happens is somebody gets on the phone
9 to somebody they know, all unofficially now, in outsider
10 channels, and that route is scrubbed.

11 What a friend of mine proposed, and actually a
12 relatively erudite internet consultant, someone I really
13 respect on these issues, proposed, and this is just a
14 starting point for discussion, an international clearing
15 house of inactive blocks, which when requested to
16 announce or activate a block, Backbone could consult, you
17 know, so it wouldn't -- you know, having a block in that
18 clearing house would not necessarily mean that it was
19 about to be hijacked for Spamming, but the fact that it
20 was in that inactive clearing house would mean that the
21 Backbone or the provider would maybe do a little bit more
22 diligence in investigating the bona fides of the person
23 applying to have the route announced.

24 And that's a starting point for discussion, and
25 I'm sure other people may take it up or they may think

1 it's a bad idea, but that's the idea we came up with.

2 MR. FRANCOIS: How prevalent has this problem
3 become?

4 MR. BROWER: More and more so. In fact, there
5 are probably lots of legacy or zombie blocks out there
6 right now that are undiscovered, just because frankly
7 it's very tedious investigative work that's required and
8 it's often not the sort of investigative work that
9 technically skilled people are adept at, you know? It's
10 not all about octets and stuff like that; it's about
11 forged letterheads and what somebody's real phone number
12 is. So, it's actually more forensic detective work,
13 honestly, than IP-based stuff.

14 MR. FRANCOIS: So, once someone has control of
15 this block, just how many IP addresses do they now
16 control?

17 MR. BROWER: Well, what is the exact number in
18 a slash-16, Michael?

19 MR. RATHBUN: 65,000-some-odd.

20 MR. BROWER: A large number.

21 MR. FRANCOIS: And with the approximately
22 65,000 IP addresses that they have in that block,
23 generally how much -- what damage can they do from a
24 Spamming point of view? How much spam can be sent before
25 it gets shut off?

1 MR. BROWER: Once you have that resource,
2 there's any number of things you can do. You can host --
3 spam-vertise -- you may advertise --

4 MR. FRANCOIS: Speak into the mike, please.

5 MR. BROWER: You may -- ooh, that was too
6 close. You may spam-vertise a given domain from outside
7 of your hijacked network and then of course find that
8 it's virtually impossible to have that advertised site
9 taken down because you control the slash-16. That's one
10 obvious use. And it also, by the way, there are other
11 obvious giveaways here, and typically you'll have an ASN
12 that you control a slash-16, you have an ASN, you're only
13 announcing 1/24. That kind of makes you curious, you
14 know, as an administrator.

15 I mean, so the point is that once these
16 problems come up they're not hard to find, but if your
17 question is how valuable is that resource, immeasurably
18 valuable. I mean, it gives the Spammer basically control
19 of his own network. And there's no upstream in many
20 ways.

21 MR. FRANCOIS: So, short of this repository of
22 deactivated IP addresses or blocks, what are some short-
23 term interim steps that can be taken to kind of guard
24 against this and who needs to take those steps?

25 MR. BROWER: This particular problem, I think

1 the largest issue that needs to be addressed, and this is
2 an issue of personnel and income, frankly. As we know,
3 providers, as an industry, many of them are severely
4 squeezed for money right now. They've been involved in a
5 race to the bottom, competing only on price for so long,
6 that many of them are operating on razor-thin margins.

7 And as a result, they cut in terms of doing
8 diligence, investigating prospective customers, doing
9 checks on addresses, things of that nature. So, you
10 know, I hate to say this, but raise prices, from a
11 practical standpoint, and compete on quality, rather than
12 price. And I've been making this case for a long time,
13 and of course it's very easy for me to say, you know, I
14 don't control a corporation that's running on one-cent
15 margins.

16 But it seems to me doing diligence, actively
17 investigating, to the best of your ability and with
18 available resources prospective customers in every
19 respect is very important.

20 MR. FRANCOIS: Thanks.

21 MR. BROWER: You're welcome.

22 MR. FRANCOIS: Now I'm going to Dr. Hancock,
23 Dr. William Hancock from Cable & Wireless, who is going
24 to give us a glimpse into the future of some of the
25 techniques and what's coming down the pike for spam. And

1 security weaknesses.

2 DR. HANCOCK: Thank you, Renard. That's like
3 calling Godzilla a lizard, so we'll see how it goes from
4 there.

5 In the past, we have the internet, this is a
6 picture of it in 1988. Back then, mail relays and
7 different types of mechanisms to move things around, the
8 biggest spam you had was the announcement of a seminar at
9 Bell Labs or something like that. And this is a current
10 picture of the internet today.

11 **(Laughter).**

12 DR. HANCOCK: This is actually off the Bell
13 Labs' website, and this is a picture of only the United
14 States. And one of the little endpoints of those little
15 lines over there could easily be a mail server. This one
16 here I'm bringing up for a point that I'm going to make
17 here in a minute. What you see at the very bottom bar is
18 Windows 3.1; the very last bar over there is Windows XP.
19 Windows 3.1, approximately three million lines of code;
20 Windows XP, approximately 45 million lines of code.

21 There's a known statistic in software
22 engineering that states that basically there are ten bugs
23 for every thousand lines of code. And it's probably much
24 worse than that, but that kind of gives you an idea to
25 think about, because one of the ways that we're going to

1 see spam spread in the future is the exploitation of bugs
2 on an operating environment.

3 Let me give you a very brief example of that.
4 On January 25th, the internet was hit with something
5 called slammer. Slammer basically took advantage of an
6 exploit on ports 1434 and 1433 of the UDP protocol based
7 upon a bug in the Microsoft sequel server. That bug was
8 fixed approximately seven months earlier; there was a
9 patch available. Since that time, approximately 450,000
10 servers were exploited with that particular whole in that
11 bug. The slammer worm that propagated around the
12 internet had a payload that did nothing, but it did gain
13 complete access to the machine. That payload could
14 easily have deposited a mail relay server, very easily.

15 So, what you're seeing in that situation with
16 the slammer worm on January 25th, was that it was a band
17 width consumption attack using a bug, a single bug, on a
18 particular product, on a particular Windows platform.
19 That was actually fixed, but people didn't put the patch
20 in.

21 What's important about that is that Spammers
22 are already starting to create tools to exploit these
23 kinds of things, where they can actually send to you a
24 mail relay server, even if you're not running one. And
25 the result of that is tools like worms like slammer allow

1 the opportunity to go back and take advantage of bugs in
2 very large and very complex operating environments such
3 as Windows XP, Linux Server, so on and so forth.

4 So, it's important to understand that as long
5 as we have complex environments we have complex software,
6 we continue to have buggy software. We have the
7 opportunity for infiltration into the machines, and as
8 long as that exists, when you start using things like
9 worms and trojan horses to transmit the data, the
10 opportunity to infiltrate the machine and deposit malware
11 is very, very good.

12 Everybody happy yet?

13 **(Laughter).**

14 DR. HANCOCK: This little statistic over here
15 is from CertCC that basically shows that between 1998 and
16 2002 the number of attacks jumped from approximately
17 1,928 attacks to well over 86,000 attacks in 2002 alone.
18 Now, these are the documented attacks, and it's estimated
19 that this is only 3 percent of all the attacks you see on
20 the internet.

21 More importantly, these are the number of
22 vulnerabilities that have appeared, just in a single
23 year, and the vulnerabilities are ways that you would use
24 to infiltrate an operating system and application or a
25 system to deposit malware, whatever that may be. And it

1 could be something as simple as a password grabber, or it
2 could very easily be a mail relay system.

3 Now, I particularly like this particular chart.
4 This is one that Rich Pethia (phonetic) puts up from
5 CERT. And what you see in the bottom left-hand corner is
6 starting approximately 1988, going all the way up to
7 2002, the sophistication of a security attack on a
8 computer system. So, as you see over time, the attacks
9 get more and more sophisticated, and frankly, they have
10 to, because the operating environments, the applications
11 and everything else are getting more and more complex.
12 That dotted line that you see, going from the top left-
13 hand corner, going down to the lower right-hand corner,
14 is the intellect of the attacker.

15 **(Laughter).**

16 DR. HANCOCK: So what you're seeing is very
17 sophisticated attacks being launched by morons, okay?

18 **(Laughter).**

19 DR. HANCOCK: And, frankly, I've got statistics
20 to back that up.

21 **(Laughter).**

22 DR. HANCOCK: We find that on our networks and
23 all that we operate a very, very large multinational
24 network. We find that the bulk of our attacks happen
25 between 4:00 on Friday evening and 9:00 on Sunday. And

1 80 percent of them are launched by kids, because most of
2 them don't have a date and don't know what to do that
3 weekend.

4 The bottom line is, though, that it means that
5 those people are able to download very sophisticated
6 tools from the internet, use those sophisticated tools to
7 launch zombie networks to go back over and infiltrate
8 other machines without themselves having the intellect to
9 know what they're doing. In fact, I've been involved in
10 over 600 prosecutions and I can tell you categorically
11 every time we run into a kid they have no clue what
12 they're running. Very rarely do they understand the tool
13 that they downloaded and what that tool actually does.
14 And as a result of that, spamming somebody is becoming
15 easier and easier.

16 We were recently involved in a situation where
17 there was some spam going on, and it was a bunch of
18 teenagers who had downloaded tools and were spamming
19 other people in their school. And they were doing it for
20 money, and the result of that meant that they didn't know
21 what they were doing. All they knew was that they ran
22 the tools a certain way, provided the spam in a certain
23 way, the next thing you know, they made money out of it.
24 And, you know, there are ways for other people to get
25 their allowance, but this one worked rather well for

1 them.

2 So, what's the entry point cost of making spam?
3 Basically a PC, some software you can download and a
4 network connection of some sort. It doesn't take a lot
5 of money to become a Spammer. It does not take a lot of
6 money for someone to get into the business. This makes
7 it a very low entry point. One of the big things about
8 cyberwar, if you ever study cyberwar concepts is that
9 cyberwar basically says it's non-lethal warfare. You
10 don't kill people, but you can make their life very
11 miserable from an economic perspective. You can disrupt
12 all kinds of economic factors involving a company,
13 involving an individual.

14 What's important about this particular thing is
15 that it doesn't cost much to get into the spam business,
16 and yet you can generate fairly good revenue. This means
17 as long as that matrix exists, you can legislate it all
18 day, you can try to put in technology all day, but as
19 long as the money keeps flowing, someone's going to
20 figure a way around it.

21 The core span need of course is to make a
22 server out there for you. Basically right now people use
23 servers that are in existence that someone has brought
24 up, either accidentally or intentionally, whatever the
25 case may be. But the bottom line is that you're looking

1 for a server, you're harvesting addresses, you're going
2 to use those servers either as an open proxy, open relay
3 or in some cases a direct connection, if you're using
4 different types of protective IP addresses, or if you go
5 back and scan IP addresses. But in all cases, you have
6 to have a server to make it go out the door.

7 The biggest thing also that Spammers have to
8 do, they have to evade capture. That's one thing to sit
9 down and say gee, we'd like to go back and spam, but you
10 have to be able to evade being caught and evade that your
11 server, when it is caught, you can go someplace else and
12 be able to go back and spam. Because of that, you have
13 to be agile and you have to be mobile. And that means
14 that the need to move around is a very critical part of
15 becoming an effective spammer in the future.

16 Now, this brings up the upcoming methods. One
17 of the methods we starting seeing very recently is of
18 course the ability to use what is called a trojan, if you
19 will, a trojan horse type of application, which comes in,
20 basically attacks a system, and then launches itself
21 inside the system, providing a server capability. That's
22 one way. And this can be done through a variety of
23 methods. There's ways to do it via hacking, you can just
24 go back and hack it, use a known back door, use a known
25 hole like the slammer did, and then deposit the server

1 capability into that machine.

2 Now, what that translates to is that everybody
3 who has a machine that's connected to the internet and
4 according to the Internet Society as of last month, there
5 are 655 million user accounts. That means that anyone
6 with a PC out there, even if they're not running e-mail
7 whatsoever, could be attacked, could have a server
8 imbedded on their machine, against their will, and then
9 that server used as a spam relay site.

10 And, in fact, there's at least four programs
11 running around the internet that do exactly that. And
12 that means that you don't have to use an open relay, you
13 don't have to go back and use an open proxy, you yourself
14 are depositing that e-mail server as part of a package
15 when you go back and bust their machine.

16 As a result of that, you can set up what's
17 called spam distribution networks, very similar to what
18 denial-of-service-attack people do with zombie attacks.
19 Most of you folks have probably heard about denial-of-
20 service attack. How many of you have children? How many
21 times you go into the potty and you find that it's full
22 of toilet paper and a plastic truck?

23 **(Laughter).**

24 DR. HANCOCK: That is a denial-of-service
25 attack.

1 **(Laughter).**

2 DR. HANCOCK: A distributed denial-of-service
3 attack happens when they bring 12 of their friends over.

4 **(Laughter).**

5 DR. HANCOCK: So, it is not a very
6 sophisticated attack, it doesn't take a lot of logic to
7 do it, it doesn't take a lot of intellect and it's not
8 that hard to do because it sucks up bandwidth. If you
9 suck up the bandwidth, there is no way that anybody can
10 get to what you're after. In the case of spam, by using
11 the same distribution methods that are used right now to
12 distribute zombies or basically small pieces of code that
13 go all over the network, you can now go back over and
14 distribute these trojans and basically provide an SMTP
15 service capability on unsuspecting machines.

16 So, a lot of people want to say, oh, okay,
17 well, how does it work. Well, basically the first thing
18 you do, somebody sits down there and they create the
19 trojan horse program. And then they also go back over
20 and create a worm. Okay? Now, when the worm comes up,
21 the worm basically has a payload in it and it has some
22 methodology of replicating itself.

23 Well, let's understand what that means. Code
24 red, when it came out in 2001, basically took
25 approximately 37 hours to replicate itself around the

1 internet. The slammer worm in January of this year took
2 eight minutes. Everyone get that? Thirty-seven hours to
3 eight minutes in less than a year and a half. That's
4 important, because it means that the propagation
5 capability of a malicious worm that contains something
6 that will go back over and infect networking resources is
7 very, very easy to do with current technology and current
8 science.

9 Now, once these zombies are all out there and
10 they're all positioned, they're ready to go, then the
11 person who operates the spam at that point goes back over
12 and creates the evil e-mail. And then at that point they
13 can distribute the evil e-mail of course over to the
14 network that's out there. The network at that point then
15 goes back over and attacks the poor, hapless end-user,
16 who ends up getting their mailbox full. And this is the
17 sort of thing that happens and all of this is known
18 science. It is not that difficult to do.

19 So, as we look at issues with this sort of
20 approach, basically what you've got to have is automated
21 distribution. We call this AML for autonomous malicious
22 logic. The purpose of this is basically using the same
23 techniques that are used for denial-of-service attacks to
24 go back and distribute zombie networks, now you're
25 distributing AML-oriented SMTP networks that can then be

1 called upon, they can be shared. You can distribute
2 thousands of these in an hour. It doesn't take very long
3 for this sort of thing to get out there, because people
4 do not adequately patch their systems because the systems
5 have a great deal of code, because they have bugs,
6 because there's all kinds of ways to infiltrate and
7 infestate the systems.

8 Legislation is not a problem, because when
9 we've legislated all day long, they just go off shore. A
10 good example of that is viruses. How many legislative
11 things have we seen attended to viruses and how many has
12 it stopped? Every month there's approximately 250 new
13 viruses that appear. It's a billions and billions of
14 dollar business. As a result of that, there is a money
15 flow; there are reasons for viruses to be created. I
16 also find it very interesting that many times new viruses
17 seem to appear towards the end of a sales quarter, but
18 that's a different issue.

19 **(Laughter).**

20 DR. HANCOCK: Go back and look at it yourself.
21 And in the situation, as we can go back and legislate it,
22 but what happens is when we pass legislation in the
23 United States against spam, we're going to turn right
24 around and see it getting broadcast and being taken care
25 of internationally. A lot of links in third-world

1 countries and folks that are just coming around to the
2 internet and very, very large organizations and things
3 like China, they don't have protective capabilities, they
4 don't have ways to go back and stop this and they may not
5 know how. You start parking a zombie network in those
6 types of environments, and the spam situation
7 internationally gets worse, and legislation is not going
8 to stop it.

9 Problems that we're going to have to think
10 about the next five years is that most of us are going to
11 go mobile. If you're not mobile already, you're going to
12 get there. And that's through 3G cell phones, through
13 Wy-Fy hot spots. There's all kinds of wireless
14 technology. Saying that we're not going to have spam
15 problems in these types of technologies is ridiculous,
16 because we're already starting to get them now, okay?

17 What's going to happen in the future is that
18 your personal cellular device, your cellular device will
19 also be connected to things like Wy-Fy telephones. As a
20 matter of fact, Cisco announced one yesterday -- the day
21 before yesterday, I believe. And you're going to find
22 these kinds of technologies out there where the phone
23 becomes your local area network connectivity appliance
24 with an IP address and simultaneously can be your cell
25 phone when you get out into the world running around.

1 That means that that device has an IP address.
2 You can actually download to these things, because they
3 run in microkernel, unix, linux or microkernel Windows
4 environment, a very small e-mail relay. So, you may very
5 well find that your phone is getting very fat in your
6 pocket because it's filling up with e-mail because it's
7 relaying it out to other phones in the area.

8 So, why do we need spam protection? I always
9 put this up as my favorite little picture. That's
10 because it's my 13-year-old. This picture was taken on
11 Sunday. That's his cat.

12 **(Laughter).**

13 DR. HANCOCK: In reality, that's a full-grown
14 Bengal tiger named Savannah that lives down the street,
15 so he plays with her off and on. Notice the satisfied
16 look on her face from eating the previous Spammer.

17 **(Laughter).**

18 DR. HANCOCK: And the point being is very
19 simple, is that my son at age six has grown up with a
20 proper geeky lifestyle. In fact, when he was born, they
21 handed him to me and I said welcome to the world, my son,
22 I'm your father, and COBAL sucks.

23 **(Laughter).**

24 DR. HANCOCK: And I have this on videotape. I
25 actually did that.

1 **(Laughter).**

2 DR. HANCOCK: My son has grown up very, very
3 good in the geeky lifestyle. He has the proper 2.3
4 computers in his bedroom, and of course with a T3
5 connected in the house, my son is well equipped to go
6 back and deal with internet capability. It helps to work
7 for a carrier.

8 **(Laughter).**

9 DR. HANCOCK: The situation is, folks, is that
10 my son also came in at the ripe age of six and said,
11 Daddy, what is a penis? And I said why? And he said
12 someone sent me an e-mail where I can make mine bigger,
13 and I thought great, this is what I need to hear right
14 now.

15 **(Laughter).**

16 DR. HANCOCK: Although lately he's been asking
17 about breasts and it bothers me a bit. The situation is
18 that these kids get this stuff. They get it at school;
19 they get it in high school; they get it all over the
20 place. Well, to adults, it's somewhat of an irritant; to
21 kids, it really sociologically causes them some very
22 serious problems. And, so my major reason why I am very
23 much anti-spam and why I spend a great deal of my time
24 worrying about it, stopping it, scanning for it and
25 finding it and killing it dead, is because of my son who

1 likes to hug a tiger. Thank you very much.

2 (Applause).

3 MR. FRANCOIS: Thank you, Dr. Hancock. We are
4 going to take questions from the audience now.

5 MR. HUSEMAN: Well, we have one quick written
6 question.

7 MR. FRANCOIS: Okay.

8 MR. HUSEMAN: The panelist mentioned the
9 numbers 402,000 for the number of new open relays and
10 open proxies per day, are those new open relays per day
11 or newly discovered open relays?

12 MR. SERGEANT: Newly discovered.

13 MR. HUSEMAN: Newly discovered, so they were
14 already existing? Okay, thank you.

15 MR. FRANCOIS: How about over there? Yes?

16 UNIDENTIFIED SPEAKER: Too many questions to
17 ask and not enough time.

18 MR. FRANCOIS: How about pick one? The
19 shortest one.

20 UNIDENTIFIED SPEAKER: In speaking of honeypots
21 and receded e-mail addresses, we've done that many, many
22 times and we never could figure out how they found that
23 address. Is that like from dictionary Spawning? Also
24 there's been a sudden and very steep increase in the
25 amount of spams that come that are like numbers separated

1 by equal marks. There's no text in the spam at all.
2 There's no subject line or anything. It's all just
3 characters separated by equal marks, and someone told us
4 this was an e-mail to find out if our mail server was
5 compromisable or had been compromised. Can anybody speak
6 to that?

7 MR. FRANCOIS: Mr. Rathbun.

8 MR. RATHBUN: Well, some of the ones that you
9 get with what would sound like to be encoded probably
10 Asian language sets, I get probably 45 to 50 spams a day
11 that are in Chinese or Russian and they look that way.

12 MR. SERGEANT: Yeah, that sounds like quoted
13 printable.

14 AUDIENCE MEMBER: Quoted printable.

15 MR. FRANCOIS: Other questions? Anybody?
16 Okay.

17 AUDIENCE MEMBER: Thank you. We know that data
18 has overtaken voice over normal telephone lines. Do we
19 have any statistics on how many e-mails per day are
20 actually being sent, either in the U.S. or worldwide?

21 MR. SERGEANT: It's about -- for our corporate
22 customers, it's around about 40 e-mails per day, per
23 user.

24 MR. FRANCOIS: Let's go -- any questions --
25 right here, in the middle. Hang on, and let's get you a

1 microphone. And give me time to repeat part of the
2 question, as well.

3 MR. IVERSON: I'm Al Iverson (phonetic) from
4 Digital River. I actually used to work for MAPS and open
5 relays are something that I'm pretty familiar with. One
6 thing I'm kind of wondering, any of you folks, especially
7 from a provider perspective, do you run into any open
8 relay operators that absolutely defend their right to run
9 an open relay and won't do anything about it? Obviously
10 Michael knows I'm thinking of somebody named John Gilmore
11 --

12 **(Laughter).**

13 MR. IVERSON: -- who I've come to realize that
14 was somebody we ran into where he wanted to sue everybody
15 who wanted to block spam from that relay.

16 MR. FRANCOIS: The question is from a provider
17 perspective have they run into anyone who operates an
18 open relay that defends their right to run an open relay.

19 MR. BROWER: Well, I have run into maybe one or
20 two people over the course of working at Earthlink that
21 have felt that way, but we have a policy to uphold, we
22 can't allow spam on the network and unfortunately, we
23 just can't allow it. I don't really understand why
24 someone would be so adamant in keeping their relay open.

25 MR. FRANCOIS: And what were some of the --

1 briefly some of the arguments that they used to justify
2 keeping it open?

3 MR. BROWER: The one I can remember would be --
4 it was just kind of silly. They did not feel like they
5 should have to change it. They had it set up from the
6 box the way the actual software was set up, it was open
7 for relay when they installed it, and he didn't feel like
8 he should have to change it.

9 MR. FRANCOIS: Michael, it sounded like you
10 wanted to say something.

11 MR. RATHBUN: From the standpoint of shall we
12 say a doctrinal or a philosophical stance, we don't
13 really see that too much. Mostly it's either just
14 planting your hooves because you don't feel like somebody
15 else should tell you how to run your system, or the one I
16 heard most recently was that nobody had the guts to go
17 and tell the CEO that he had to reconfigure his laptop.

18 **(Laughter).**

19 MR. FRANCOIS: Any other questions? Way, way
20 back in the back.

21 AUDIENCE MEMBER: Can you hear me? Can you
22 hear me now?

23 **(Laughter).**

24 AUDIENCE MEMBER (Partially audible): -- Double
25 Click. This kind of goes to the open proxy question. I

1 think by now we've all heard some variation of this
2 story, I was in a hotel or I was in Starbuck's and I just
3 turned on my computer and my wireless card and boom, I'm
4 on the net. And that's been my experience, too, for \$3
5 or \$4 -- we've all heard about the Pringles can --
6 (inaudible) -- wireless card that pick up connectivity
7 three miles away. And I tried the experiment from my
8 house, you know, I was easily hypothetically on five or
9 six people's networks without much work. Now, what kind
10 of a threat does this pose, if I was -- (inaudible) --
11 Linux box with an MDA built in, you know, is this a real
12 threat and are we finding that kind of connectivity to be
13 Spammer's next choice?

14 MR. FRANCOIS: The question is what kind of a
15 threat is wireless connectivity and is this the next
16 Spammer choice? Takers?

17 DR. HANCOCK: It's a huge problem already.
18 We've got an awful lot of wireless capabilities running
19 around within the company called Cable & Wireless for a
20 reason I guess. One of the situations I keep running
21 into is that even our own folks put up wireless networks
22 and sometimes inadvertently leave something open and
23 someone wanders by in a car or driving or some nonsense
24 like that and they're on.

25 The biggest problem that we're seeing right

1 now, though, is that with the predominance going to
2 wireless and especially 802.11A, and 802.16, which just
3 announced two months ago. 802.16 is a metropolitan area
4 wireless which allows you anywhere from 54 megabytes up
5 to 100 megabits, and allows it over a 30-mile range, and
6 so, therefore, the limited range of 82.11 of 825 feet is
7 about to go out the window. And with that kind of
8 capability, you now have a metropolitan wireless
9 capability that anybody can tie into. And that means
10 that you don't have to have wire; you can obviate the
11 local loop; there's all kinds of ways to easily connect
12 to this. And the base security at level two at these
13 things to connect in and authenticate is a joke.

14 As a result of that, it's very easy to connect
15 to these kinds of networks and use them for legitimate
16 connectivity with an IP address and become a relay of any
17 kind. So, if you add that into the capability of also
18 assigning zombie code and things like that to these kinds
19 of machines, it's going to be a very large problem.
20 We've already got the problem now of just people
21 illegally using those kinds of networks, using them in an
22 illicit way as well is going to be a real problem.

23 MR. FRANCOIS: One last question. Anybody? A
24 hand back there.

25 MR. SOUDER: Hi, Doug Souder, from Hunting

1 Software. In the session where we were talking about
2 harvesting e-mail, somebody said that that was the air
3 that keeps Spammers going, and I was just wondering if we
4 could somehow get the upper hand on the open relays and
5 the proxies. Do you think it would have a similar
6 impact? Is this the air sustains these Spammers?

7 MR. FRANCOIS: The question is how can we get
8 the upper hand on open relays and open proxies and is
9 this the air that sustains the Spammers? A very short
10 answer.

11 MR. BROWER: I have a very short answer.

12 MR. FRANCOIS: We'll take it from two, Adam and
13 Matt.

14 MR. BROWER: I hope mine is shorter, and the
15 only time I'll ever say that.

16 **(Laughter).**

17 MR. BROWER: I've been reading too much spam.
18 I think the technology is the answer and sociology is not
19 the answer. So, I mean, and I'll take this opportunity
20 to be entirely off topic for this panel. I believe
21 firmly in DNS-based IP blocking, combined with rigorous
22 white listing as the only solution to this problem.

23 Now, there are ways to get around it, but as
24 far as I can see, going forward, that's the only thing
25 that will work.

1 MR. FRANCOIS: Matt?

2 MR. SERGEANT: It's an arms race. We will --
3 you know, we will beat the open proxies problem into
4 submission, hopefully, and there will become other ways,
5 as Bill has described, that they will find other ways of
6 distributing their stuff.

7 MR. FRANCOIS: One quick question from me for a
8 yes or no answer from the panelists. Basically, should
9 the government in terms of -- we talked about companies
10 scanning their proxies and servers. Should the
11 government also get involved in scanning for open proxies
12 and open relays? Yes or no.

13 MR. SERGEANT: No.

14 UNIDENTIFIED SPEAKER: Waste of time.

15 MR. FRANCOIS: So, we've got a no, no, a waste
16 of time and?

17 UNIDENTIFIED SPEAKER: No. In case you didn't
18 hear me.

19 MR. FRANCOIS: All right, so everybody agrees
20 now, and I wish we would have had more time to go into
21 the reasons why, but we are at the end, and I have a few
22 announcements that I need to make for the end of the
23 panel.

24 First, on May 16th, the Federal Trade
25 Commission and its Southwest partners in the Netforce are

1 going to make an announcement and have a press event in
2 Dallas, Texas concerning open relays, so please stay
3 tuned.

4 Administrative announcements, today is the end
5 of day one, and we want to thank you all for braving the
6 cold temperatures, the bright lights and the long lines.

7 **(Applause).**

8 MR. FRANCOIS: It's been a very productive day,
9 and I just want to make three quick announcements. One,
10 as always, it's about your name tags. Panelists, hang on
11 to your name tags if you're going to be back for the
12 duration or tomorrow or any day. If you have one of
13 these peeling name tags, then you will have to get
14 another one tomorrow. The one you have now will not be
15 good for tomorrow. And everybody, regardless of whether
16 you are a panelist or an audience member, will have to go
17 through security.

18 Second, I thought many of you were crazy when
19 you said it's too cold in here, but I can't feel my feet.

20 **(Laughter).**

21 MR. FRANCOIS: And until I become a
22 Commissioner, they're not going to change the
23 temperature, so dress warmly tomorrow, because they've
24 told us they can't move the temperature up or down.

25 Finally, tomorrow morning we convene with

1 remarks from Commission Thompson at 8:15, and our panel
2 will be the Economics of Spam at 8:30. Thank you very
3 much, and we look forward to seeing you tomorrow.

4 **(Whereupon, the hearing was adjourned).**

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

C E R T I F I C A T I O N O F R E P O R T E R

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

1 DOCKET/FILE NUMBER: P024407

2 CASE TITLE: SPAM PROJECT

3 HEARING DATE: April 30, 2003

4

5 I HEREBY CERTIFY that the transcript contained
6 herein is a full and accurate transcript of the notes
7 taken by me at the hearing on the above cause before the
8 FEDERAL TRADE COMMISSION to the best of my knowledge and
9 belief.

10

DATED: MAY 19, 2003

11

12

13

SONIA GONZALEZ

14

15

16

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

17

18

I HEREBY CERTIFY that I proofread the transcript for
19 accuracy in spelling, hyphenation, punctuation and
20 format.

21

22

23

SARA J. VANCE