OFFICIAL TRANSCRIPT PROCEEDING

FEDERAL TRADE COMMISSION

MATTER NO. **P024407**

TITLE **SPAM PROJECT**

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

DATE **MAY 1, 2003**

PAGES **1 THROUGH 324**

FTC SPAM FORUM -- DAY TWO

SECOND VERSION

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

FEDERAL TRADE COMMISSION

I N D E X

Economics of Spam	Page 5
Blacklists	Page 111
Best Practices	Page 183
Wireless Spam	Page 257

P R O C E E D I N G S

- - - - -

MR. HUSEMAN: We want to go ahead and get started this morning. Thank you all for arriving back for day two.

Before we begin, I just want to make a few housekeeping announcements. Remember, if you have a cell phone or other device that beeps, make sure to turn it off, please.

Remember that the exits are directly behind you and then out towards the front where you came in.

Again, we would like to thank the companies who have provided us refreshments this morning. Those include AOL, AT&T Wireless, EarthLink, ePrivacy Group, Microsoft, SpamCon Foundation, Words to the Wise and Yahoo!.

Before we begin day two, I would like to introduce Commissioner Mozelle Thompson, who will start off the day by giving us introductory remarks. Commissioner Thompson became a Commissioner at the FTC in 1997. He's Chairman of the OECD's Committee on Consumer Policy, where he leads the United States delegation, and during his time at the Commission, he has been very involved in technology, privacy and other information practices, including the issue of Spam, and he's done a

great deal of important work in those areas.

And, just specially, we would also like to thank him from the perspective of putting on this forum. He has provided us with a great deal of valuable advice and input in making this event possible. So, we would like to thank him in that regard as well.

I now introduce Commissioner Mozelle Thompson.

(Applause.)

COMMISSIONER THOMPSON: Good morning. Welcome all of you, and for those of you from out of town, welcome to allergy season in Washington.

I wanted to tell you how happy I am to see you all here at the second day of the FTC's Spam Workshop. As you know, my name is Mozelle Thompson, and I'm one of the Commissioners here, and I hope that you -- first of all, I think you should give yourselves a round of applause, because -- for just being here, attending and participating, because I think that in the future we'll look back on these three days as one of the most significant events, international events that deals with the subject of Spam. So, I want to thank you all for being here.

(Applause.)

COMMISSIONER THOMPSON: You know, one of the principal purposes of having this workshop, in case it

wasn't that clear, is to provide the Commission with the best and latest information about Spam and the problems of unsolicited e-mail and that I hope all of you will learn as much as I expect to learn from the events of these three days.

Now, yesterday we attempted to define what Spam is, other than the fact that it's a very popular meat out in Hawaii, and I think that that definition was a diverse definition that we heard yesterday when we start to consider what types of communications we should put under the title "Spam" and what benefits and problems they pose for consumers, businesses and governments. We also heard from experts about the mechanics of how Spam works.

Now, today we'll continue our work by discussing the economics of Spam. I hope after this morning, we will all become more knowledgeable about the real costs of unsolicited commercial e-mail. And these costs go well beyond the simple cost of sending a message. They also include the costs of individuals reading and disposing of unwanted e-mail and the cost of carrying Spam on a network as well as potential lost opportunities that would -- of bandwidth that could be provided for perhaps more useful and important purposes.

We'll also talk about the market and competitive forces that can affect the value we ascribe

to Spam. In thinking about all these costs, however, I ask that you also consider the larger costs to the marketplace to the extent that unsolicited e-mail can undermine consumer confidence and feed public distrust of the internet.

Finally, we will finish today's sessions by looking forward at best practices and the next frontier, or what many would say is already the current frontier, the wireless marketplace.

So, to assist in our discussion, I'm reminded that this might be an illustration of the old adage what the problem is depends on where you sit, and I'm sure that our panelists today will give us a lot of insight as to how we should think about Spam.

So, thank you very much for being here, and without further delay, we have our panel.

(Applause.)

MR. FRANCOIS: Thank you, Commissioner Thompson, for not only your remarks but for your efforts in the FTC's work on Spam.

My name is Renard Francois. I'm a staff attorney with the Division of Marketing Practices at the Federal Trade Commission and also pitching in a little bit with the Spam Forum. So, we have a distinguished panel here, and as Commissioner Thompson said, we are

going to talk about the costs and benefits of Spam, and part of this panel, what we're going to do is talk about dollars, but we're also going to expand the term of "cost" to include the potential impact on e-mail marketing and the potential impact on e-mail as a means of communication, but we'll also include in the definition of "cost" opportunity costs and loss to a business' reputation that unsolicited e-mail may have.

One of the things that we recognized yesterday was -- we focused on Spam and a lot of it on falsity and people who intentionally manipulate systems to try and maintain an illusion of anonymity, try and maintain anonymity by falsifying where the e-mail is coming from, but one of the things that we struggled with in our conference call and the issues that we'd like to at least be aware of throughout the panel is that it's not just deceptive Spam that affects many of these panelists, and it's not just deceptive Spam that affects e-mail as in e-mail marketing and as a means of communication, but it is the volume as well.

So, to some degree, I don't know if we are going to get into a lot of distinctions between legitimate bulk marketers and bulk marketers who engage in deceptions and falsity.

One of the things that we want to start out

with that I've sent all the panelists is Mail Shell, a company who was kind enough to forward us a study that they had done, and copies of the study are outside in the back on the table, and I think there's also a representative here who may answer any questions that you may have about it, but they did a Spam Catcher Attitude Survey, where they surveyed 9,000 -- approximately 9,321 individuals about their attitudes towards Spam, and out of the 1,118 responses that they received, I think one of the things that we'll start the conversation with is, that leapt out at me, is that 8 percent of people that use disposable e-mail addresses, which we presume are somewhat tech-savvy and maybe not the everyday, average consumer, but approximately 8 percent of them have indicated in the study that they have made purchases based on the Spam that they receive. And I just want to throw that out to some of the panelists to see what their responses and reactions are and probably direct it specifically toward Mr. DiGuido, CEO of Bigfoot Interactive, and Ms. Laura Betterly as well, and then probably Laura Atkins.

MR. DiGUIDO: Thanks, Renard.

Just to make it very clear, the role of Bigfoot Interactive in the marketplace today is we work with many of the Fortune 2000 companies in the industry who are

reputable providers of goods and services to the economy. These are folks who are using e-mail marketing as one of the ways in which they communicate to their target audience and to their current customers, with their information, with services that they find for us.

What's interesting about this study that 8 percent of folks actually purchase something via Spam is if you think about the role of advertising in the U.S. marketplace today, $228 billion spent annually in the year 2003, forecasted, by marketers selling products to customers, customers and/or prospects, the e-mail marketing channel isn't just another channel of distribution in terms of ways in which you can intersect your product with a potential prospect.

When you think about the average newspaper or the average television station or the average magazine, while you're going through that publication or through that television station, you're being inundated with all types of commercial messages, and you're browsing. You pick certain messages and you say that's of relevance to me, and others that are not relevant to me. You take action on those that are relevant, don't take any action on those that are not.

The e-mail delivery channel is a similar channel. So, it's not surprising that a percentage of

folks who are browsing, using e-mail, have been exposed to products and services that are of interest to them and that they have actually taken those actions. It's consistent with other media that are out there. So, as much as we would like to say that, you know, everything we receive from an advertising standpoint is something we solicit, we are actually being targeted by marketers from an advertising perspective based on our profile, based on our interests and are exposed to advertising that sometimes we're interested in and we do take action. So, I think the e-mail channel is just indicative of that type of behavior.

MR. FRANCOIS: And before we move on to Mrs. Betterly, I just want to ask you a couple questions.

Is there any way to compare this response rate to unsolicited e-mail and compare that to unsolicited regular mail in terms of the percentage of people that receive unsolicited mail in their mailboxes, how many make purchases based on those unsolicited mails, compared to the people who make purchases --

MR. DiGUIDO: It's really tough, Renard, to do that, because where we spent most of our time with reputable marketers is having those marketers understand the profile of their potential prospect and trying to use e-mail -- and this is where the distinction happens

between e-mail and other broadcast type of media -- through the e-mail channel, the marketer is really given the opportunity to establish a dialogue. There's an exchange of information between that customer and/or prospect over preferences, so marketers are getting much more sophisticated in terms of learning more about what their customers and/or prospects want. With that type of information, they can be much more contextually relevant using e-mail versus offline channels.

So, using Spamming, by whatever media we're talking about, whether direct mail or newspapers or print or television, in that general description, there's no real data in terms of one versus the other.

MR. FRANCOIS: Okay. Also, you said that marketing was or advertising was approximately a $228 billion business, and I was just wondering, was that online advertising, advertising in general, and if it's just advertising in general, how much of the $228 billion is --

MR. DiGUIDO: Is e-mail?

MR. FRANCOIS: -- online versus -- and e-mail versus pop-ups and stuff like that.

MR. DiGUIDO: $228 billion is the total advertising marketplace. Today, the statistic we look at, the e-mail business as a business, is projected by

2006 to be anywhere from a $6 to $8 billion piece of the overall pie. So, if you think about e-mail as a communications channel, it is a relatively small percentage of the overall advertising dollars being used in the marketplace today.

However, what's incredibly important I think. I have been in the media business for 25 years and sold print advertising, broadcast advertising and so on. This is the fastest-growing channel in terms of consumer acceptance. So, there is no doubt more people -- an average of 2 million users per month going on the internet, more and more as the behaviors change, as the demographic profile of the audience change, more and more gravitating to the e-mail and to the internet channel as a primary channel of information exchange. So, it's incredibly important. It's a relatively small percentage right now of the overall advertising dollars but growing very, very fast.

MR. FRANCOIS: Do you know roughly how much the percentage has grown in the past year?

MR. DiGUIDO: In terms of advertising dollars?

MR. FRANCOIS: Yeah.

MR. DiGUIDO: It's probably doubled just in the last year.

MR. FRANCOIS: Okay.

MR. DiGUIDO: Again, amongst Fortune 2000 types of companies.

MR. FRANCOIS: Mrs. Betterly, anything to add about the study?

MS. BETTERLY: Well, I do want to just say, I'm actually in agreement with Mr. DiGuido on all points, but the one thing that really needs to be taken a look at is that he works with Fortune 500 companies -- Fortune 2000 --

MR. DiGUIDO: No, Fortune 2000.

MS. BETTERLY: 2000, I'm sorry, I apologize, and my clientele is actually more small entrepreneurial kind of guys, and they don't have an advertising budget for print or to be on TV or to get a billboard and so forth, and a lot of these guys, we pass on very good values to consumers. For example, I have a client who is a manufacturer of PCs, and they don't have an advertising budget of a Dell or a Compaq or a Gateway, and they can give a computer to a consumer, I mean, for $299.

It's kind of -- when you look at the dollars that are spent, you -- the value of what you're going to get as an e-mail marketer and going ahead and pushing it that way is a lot less expensive than going the other route. So, it actually has an entrance point for entrepreneurs to see, does that product work, is it

interesting to people? And I'm not talking about the same offers that everybody sees, you know, lower your mortgage, you know, things that are kind of customary and everybody goes, oh, God, not another one of these.

We try to look for newer guys -- I mean, I have another client who is on Social Security and has written a book about billiards, and he supplements his Social Security with a very small mailing once a month, and he's pretty high maintenance, but we love him, and you know, he gets 30 orders, and he makes, you know, an extra $200 or $300, and that supplements his Social Security. So, we're talking about real people being able to market. Now, that guy could not buy an ad anywhere else or be able to push to people.

MR. FRANCOIS: I want to backtrack for a second and then I am going to return to you, Mrs. Betterly, and forgive me if I get people confused, because we have two Lauras and a Lisa, so -- and it's been a long night, so I want to return to Al for a second and, you know, as we all know, the economy has had a downturn, and I just wanted to get your perspective on what impact a slow economy has had on the use of online advertising, and in particular, the use of e-mail marketing.

MR. DiGUIDO: Yeah, I think just to carry on the point there and to address yours, the appeal of

e-mail marketing has been the fact that the threshold, the barrier that a marketer, whether it's a small to mid-size company or a large company, can intersect between a message and its audience is probably the lowest threshold of any media out there. Not probably, is the lowest threshold. So, for that small to mid-size company to go out and run local spots on TV or radio or in print is going to be cost-prohibitive.

What has really accelerated the growth of the e-mail marketing business today is the fact that budgets are tighter. There is not a company that we deal with in the Fortune 500 or 2000 that is looking at larger budgets this year to grow sales, acquire new customers and retain their existing customers. Most of these companies are faced with tighter budgets, smaller budgets, and being asked to stimulate greater sales this year versus last year. So, they are desperate to find much more cost-effective and efficient ways to get their message in front of the consumer.

What the beneficial part of the internet is, just at this point, where their budgets are being constrained, the Internet is exploding and providing them a very cost-effective and efficient way to do permission-based contextual messaging. So, during this period of time, our business has actually grown, and the

percentage of a reputable marketer's budget that is being targeted to this area is growing exponentially.

MR. FRANCOIS: Let me return back to Mrs. Betterly and ask you just a little more specifically about your business and the type -- what you do for your clients in terms of -- how much does it cost in terms -- how much does it cost for you to take the time to craft an advertising campaign with a particular client? How long does it take?

MS. BETTERLY: Well --

MR. FRANCOIS: Just some more specifics about -- about the cost structure.

MS. BETTERLY: -- I would say in general, to actually put together a creative or an advertisement for one of our clients, we don't charge a lot. We charge $250, and we give them a couple of changes in that. We give them a big questionnaire so that we get what they're trying to achieve out of it and whatnot, and we spend time.

Now, a lot of our clients will also do that work themselves, but we provide that service, because a lot of the guys that we're dealing with are new and entering the marketplace, you know, for the first time.

I don't believe in price-gouging. I mean, we're all -- you know, I'm trying to help guys like

myself who are in business for themselves and trying to grow. We don't also charge a lot either, I mean, in conjunction -- of course, we make money with what we do, but I would say depending, you know, on how targeted we're going, because we can take our lists, which are, you know, permission-based, and we can find, for example, major markets like New York or Tampa, and we've done this with several types of -- we find broadcasts for entertainment or new shows and whatnot. I come out of the music business, so I have a lot of contacts there.

For example, we've been able to -- with a couple of pilots we've done with a few clubs, where we've been able to pack the club that they have actually not been turned away business, I mean closed for the night because they are at capacity, and people seem to be willing to get that kind of mail also, you know, telling them about events, you know, we worked with an equestrian event down in Florida, and they had their highest sales in 31 years in business.

So, we're seeing what is successful and what's not, and frankly, if I look at a campaign and I don't think it's successful or I think it's too similar to other things that are out there, I will turn down the business, because that's not what we're looking to do, is we want to keep people's permission, you know what I'm

saying?

MR. FRANCOIS: Well, let me jump in and interrupt you and ask you what do you consider to be a successful ad campaign from the perspective of response rates? I know a successful one ideally would be everybody responds to it or everybody purchases the product, but in reality, what is a response rate that you consider to be a successful campaign?

MS. BETTERLY: Well, on these broadcasts, I've actually had open-ups where people have looked at it as high as 35 percent, which is very unreal, but because we targeted and the people that were actually targeted wanted to get this information, they looked at it.

We have done some where the response rate was less than 1 percent, I mean, opening up, and that was not successful. The big thing is to test it, you know, and when you're talking about e-mail marketing and guys with not a big budget, they don't spend for marketing surveys and what are the buttons and what colors do people more indicate to mean this for them and that for them. So, sometimes it's actually reworking it several times to see where the biggest response is.

You know, you'll send out a few and see what that rate is, and you'll try another thing or another idea several times until you get what works. You know,

you do it a certain amount of times, and then you look at it and you go, well, this is not the thing, but we try to work along with everybody to see that we get that.

MR. FRANCOIS: And let me ask you, you mentioned the fact that on one particular campaign you had 35 percent open-ups. If you could explain what that means and how you all are able to monitor whether the e-mail has been opened up or not.

MS. BETTERLY: Well, first of all, we send -- well, first of all, the thing that people will see is that it's from -- and it may be events in Tampa or, you know, computer offers or whatever it is, so they kind of get an idea of what it's about, and then there's a subject line. Now, the subject line is relevant to what's inside, and if the subject line has enough information that makes people interested, they'll open up. So, your first indicator of what's what -- and also how good of a list you're dealing with, is the percentage of people that open up.

Technically, in HTML, you can put in a pixel so that every time someone opens up the mail, it will count what it is. It's just -- it's part of the technology of it.

The second statistic you have, because the goal of an e-mail is actually to get somebody to a landing

page, and the landing page is the thing that goes ahead and lets the individual decide if this is something they want to opt into -- want more information, want to purchase or whatever it is -- and that's your second percentage, is out of these guys that looked at what you sent, how many wanted more information from those?

And those are -- and then thirdly, of course, out of that, how many people converted to actually buying, et cetera and so on? And by monitoring those three statistics, you're able to tell if something is viable or not.

MR. FRANCOIS: I know this may be very difficult, and I didn't kind of put you on notice that I might ask for this, but if you could give us in a general sense -- you gave us the three classifications of numbers that you look at, if you could give us in a general sense, from your advertising campaigns, the percentage of open-ups to the percentage that go to the landing pages and then the percentage that actually purchases.

MS. BETTERLY: I would say that it's very probable, if we have a good campaign, to get anywhere from 2 to 8 percent to open-up. Now, the actual click-through itself really varies on the campaign. It really does. Like I told you, my computer offer, every

time I send it out, we end up selling 20 to 30 computers, and that's a wonderful -- you know, that's a wonderful campaign, and we're very happy with that.

But again, it's hard to say on that, and I'm not trying to be nonresponsive. It's just such a large variable.

MR. FRANCOIS: What in your campaigns do you find have the largest response rates or the most successful campaigns out of all that you advertise?

MS. BETTERLY: Things that are tech-related, like software, the computers, and the thing I think that actually does the best is the stuff related to entertainment and what is going on entertainment-wise within somebody's local neighborhood.

We did a promotion for a show that was being aired on Much Music, and we were trying to see if we could affect the Neilson ratings, and we did. Not much, but we were able to see that there was a difference in those target areas that we sent.

MR. FRANCOIS: And I also want to briefly -- go ahead.

MR. DiGUIDO: Are you mailing -- Laura, are you mailing third-party opt-in on behalf of this audience, right? You don't have your own -- these aren't house files that you're mailing to?

MS. BETTERLY: They're both.

MR. DiGUIDO: Okay. So, you're getting a better -- are you getting better click-through on house files versus third-party opt-in?

MS. BETTERLY: It depends. Like I said, the stuff that's broadcast and informational on what's going on seems to just blanketly do better, and -- because, you know, like I said, we have proven that several times at this point. Again, it just depends. I mean, we have -- you know, our collection sites are more high-tech oriented because I come out of that, so of course, my high-tech type offers do better with them.

MR. FRANCOIS: Earlier -- previously you had talked about tailoring your ad, and I just wanted to get a sense of is that something that you do, a service that you provide for your clients in terms of targeting -- I'm sorry, targeting, not tailoring, but targeting your ad, but is that something that the clients walk in the door with, we would like to advertise to these people, or how is that done?

MS. BETTERLY: It's both. It's both. It really just depends on the client. And again, there's such a diverse range of what people need and want.

Right now, we're actually doing a survey in Virginia for -- for a company that's actually a

lobbyist, and they want to ask -- they are asking three questions about what's going to affect the law, and they want people's response to that, and that will probably go out in the next week or two, and we will see what kind of response we get to something like that.

But because of that, he only wanted the State of Virginia, and the -- and this D.C. area, so that is -- again, that's just one way we can select. We can also select music lovers. I've also -- as I've told -- the audience doesn't know, but I'm also the founder of an MP3 software company, and that particular list is very responsive to very specific types of offers, musically related and so forth.

MR. FRANCOIS: So, generally speaking, about how much e-mail marketing materials do you send out on a weekly basis?

MS. BETTERLY: It depends, again, how many clients we have and what's going on. I would say on an average, 2 to 4 million e-mails a day is probably what we do. We've done more, and we've done less. It just depends on what's going on.

MR. FRANCOIS: And do you have something -- like a -- do you have a benchmark, like a percentage per million that you have to have a response rate for that is a profitable percentage or a break-even percentage?

MS. BETTERLY: Again, it depends on what the deal is, and I -- again, I'm not trying to be unresponsive. What we usually do is we charge per million on -- if we're -- so that whatever I'm mailing out, I'm going to make a certain amount, and we usually will do that versus a commission on the product, and so if we meet our threshold -- so, let's say it's like, you know, X amount per million, up to a cap of let's say 3 million e-mails sent or this many orders, whichever comes first, and then after we look at that and look at the response rate and what the commission is, we decide if we're going to run that further as a per acquisition or continue to test with the client themselves.

MR. FRANCOIS: Well, client expectations, is there any difference in terms of what you and your staff considers to be a successful response rate versus what clients walking in the door consider to be successful or are shooting for?

MS. BETTERLY: Well, everybody who comes and wants to market wants to sell as many of whatever it is they're selling as possible, and they want to make a ton of money and do very, very well. Now, is that always realistic? No, but there's two things.

Is the customer looking to sell something or to acquire a customer, because if you're talking about

acquiring a customer, you might not actually make as much money as you spent in the actual marketing itself, but now you have captured a customer and somebody who you can now target yourself and resell and upsell, et cetera and so on, like in any other kind of marketing.

So, it really has more to do with the customer's goal and what they're trying to do and what they're trying to capture in the market. If it's a one-time type of sale, like my friend who sells a book on billiards, there's nothing else for him to sell to them. So, he has to make money on that particular campaign. But other guys who have a disposable product that somebody will be buying again in three or four months and they can keep in touch with them, then it's the cost of the actual acquisition of the customer itself.

MR. FRANCOIS: Okay, Mr. DiGuido wanted to add something.

MR. DiGUIDO: Yeah, I just think from the perspective of the Fortune 1000 types of companies, today, wherever we go, ROI is something that is top of mind for all marketers that we talk to. So, in the years gone by in the advertising business, there was a -- there could be an opportunity where you weren't as tightly held in terms of accountability in terms of dollars spent. Today, it's a significant issue.

So, when marketers come to us, what they want to do is use this medium in a new way to be much more contextually relevant to that consumer and provide that consumer specifically the type of information that they need. I'll give you an example. We do a lot of work in the publishing area, Washingtonpost.com is one of our accounts. What they're trying to do in their newsletter products and deliver appropriate content to their audience, to their subscriber base. They realize that if they understand more about the preferences of those customers in terms of the types of editorial content they want, they can deliver a much more contextually relevant message.

When they do that, it becomes a much tighter relationship between the content provider and the audience and a much more fertile advertising environment for the advertiser. So, when you talk about the overall effectiveness of a campaign, the more that a marketer understands about the preferences of their audience, they can use the e-mail marketing platform as a way that they can't use any other medium in terms of targeting and relevancy.

So, our marketers will come back to us and say, again, so this segment of my audience, we got this type of open rate or this kind of click-through rate, and we

can actually track, with the vendor's permission and the customer's, all the way to a website, to a transaction.

So, the correlation between understanding the audience, understanding what the preferences of that audience are and delivering a relevant message provides a high conversion rate.

MR. FRANCOIS: And finally, to return to Mrs. Betterly, I just wanted to get a sense of, as you alluded to in the beginning, that you work on behalf of small companies, and you are not -- I just wanted to get a sense of the size of your staff and how much it -- from start-up to right now, how much you generally spend on internet service provider connections, staff, just to get a sense of the -- how large -- I don't want to say how large your operation is, but in terms of -- how cost-effective it is to engage in e-mail marketing.

MS. BETTERLY: Well, I'm very lucky in many different respects, because I have the background of being a founder of PCDJ.com, and from there I actually did a lot events in the dot com world. So, I already had a very good contact list of individuals that I had already had previous -- previously worked with and knew me and knew I always did what I said and, you know, and that was very, very helpful.

I saw the advantages of marketing via e-mail as

a founder of PCDJ, because we sold a lot of software. We had a free download. We would market similar kinds of things to that demographic, which are, you know, kids, DJs, music lovers and whatnot, and, you know, these are guys who buy music. They buy software. They like snowboards. They like, you know, cool clothes. And we saw that that was very, very effective. And although that mailing list is only about a million and it gets two mailings a week, it's always strong, and I thought that was great.

Then when I did the events, I was actually e-mailing out the invitations for these events, and these would be events attached to trade shows that are now defunct, like Web Noise and Jupiter and -- that's still around, but it's gotten a lot smaller, so I don't want to give a wrong impression there, but at that time, a lot of dot coms were willing to spend a lot of money on marketing, and we would rent out a club and get, you know, Jam Master J or Deaf Poetry Jam, and we would do this whole thing where there would be a place after a trade show for people to do their business development.

And you didn't get into an event without giving a business card, and everybody knew who I was, and I amassed this great list for events, and whenever we would have an event, we would send an e-mail, and I would get

my guest list back, and that's all we marketed to that list, and that was a great response rate.

And I thought, you know, between this and that -- and I'm looking at, like, what do we do next, because when the dot com world -- or dot bomb, depending on how you want to look at it -- kind of crashed, I was like, okay, now what do I do?

And what I did was I leveraged two people that I knew that each had a very, very good opt-in list who wanted a copy of each other's, and what I did was I got paid by getting a copy of that, and that put me in business, and then what I did was is I researched infrastructure and had a couple of friends who actually helped me start PCDJ who knew the technical end of it, because I know enough technology to be dangerous, but I can't put a network together.

MR. FRANCOIS: So, would you say a fairly low barrier economically to entering?

MS. BETTERLY: Yeah, so I would say our initial costs were about $15,000 to start, and that was last August, and that was me and two others. We're now up to nine people. We're moving out of my house into a real office space next month. The press that we've gotten, of course, has helped it grow tremendously, but yeah, that's -- and it is profitable, and it was profitable

from day one.

MR. FRANCOIS: So about $15,000 down in August. About how long did it take you before you broke even?

MS. BETTERLY: Probably by the beginning of November, we were -- broke even.

MR. FRANCOIS: Okay.

MS. BETTERLY: And we were able to draw salaries in actual fact probably in October.

MR. FRANCOIS: Okay.

MS. BETTERLY: Yeah, so that -- which is a very, very -- you know, bootstrap, startup, you know, do the best you can and whatnot and try to do it right.

We encountered some very interesting things, though, which do affect us economically.

MR. FRANCOIS: And we will get to that.

MS. BETTERLY: Okay.

MR. FRANCOIS: But I wanted to touch upon one thing that -- and talk about your costs in terms of maintenance and upgrading systems. Is that -- well, we'll save that for later, because I think I know where you're going, and we'll tackle that in a second, but I've been putting Ms. Atkins on hold for a long time, and let's get to her about the study and other things that she's heard.

MS. ATKINS: I was actually quite surprised by

the 8 percent number in the study, and then I thought about it a little bit, and I looked through, and one of my questions would be, is that 8 percent of the people who are defining Spam as mail I don't like and mail that's pornography, or is that 8 percent -- are they making purchases from companies who are sending them mail, they're defining it as unwanted mail sent from companies from whom you've purchased something before, and that was 50 percent of the respondents, but if they're purchasing something from a company that they've already purchased from before, is that the same as purchasing from random commercial e-mail advertising pornography?

And I think the numbers may need to be broken out a bit better to give us a better understanding of what the respondents are actually saying here. That's my big comment about the 8 percent number, because in that case, I'm not even sure that that really is Spam. If I make a purchase from a company and when I purchase I give them an e-mail address and I say, yeah, let me know about other offers, I've solicited mail from them.

And so while I may turn around and decide that a certain company is sending me mail that I don't want and now that's Spam, it's hard to measure the solicitation inherent in what these purchases are, not

knowing who's purchasing what and what they're actually purchasing in the survey.

MR. FRANCOIS: And what Laura is referring to is MailShell study also had a question or a list of statements and an area for consumers to agree -- the respondents to agree with, and 53 percent agreed with the statement that they consider Spam to be any unwanted e-mail from a company from whom they have purchased something. So, existing business relationship arguably, but they still consider the receipt of a subsequent e-mail to be Spam, and more than half of the respondents considered that, just for clarification.

Well, with that in mind, let's turn to the ISP folks and ask them a couple of questions, and we have got Dale Malik from BellSouth and Lisa Pollock Mann from Yahoo! in terms of, well, what is Spam and has their definition changed based on what their consumers say? And do we want to start with Mrs. Mann?

MS. MANN: So, we define unsolicited -- we define Spam to be basically unsolicited bulk e-mail, but it's actually really, really difficult to define what Spam is, and that's part of why we're all here over those three days, right, because essentially the customer tells you it's Spam, as an e-mail service provider, you have got to kind of trust the customer, right, and our point

of view is to really provide the best online experience that we possibly can for our customers.

And we actually have built things into our systems to get that kind of feedback, so when you receive an e-mail in your inbox in Yahoo! mail, you actually have a choice to click on a link that says this is Spam, and conversely if you receive a message in your bulk mail folder, you can click on a link that says this is not Spam. So, we receive a lot of that feedback from our customers.

So, it's -- we have our own definitions, everyone on this panel has their own definitions, and I think the broad definition that we often subscribe to is e-mail that is sent to individuals without their request or their consent and without a preexisting business relationship with the sender. That's kind of the broadest definition that we subscribe to.

Most important for us is to give our users the choice to be able to give us that feedback as to what they think is Spam or not.

MR. FRANCOIS: Is that a definition that you all have had for a long time or is that a definition that you all have recently, in the present, changed based on consumer response?

MS. MANN: Well, that's pretty much been

consistent from the time that we started offering e-mail, which over five years ago at Yahoo!. What has changed is not the definition of what is Spam, but rather, the tactics that people are using to get into the inbox. People are getting more and more devious. They are using more misleading, more deceptive practices. So, we have to be much more aggressive in how we are dealing with people that are trying to get in to destroy our users' online experience.

MR. FRANCOIS: Have your consumers' expectations and how you all deal with Spam changed over time?

MS. MANN: Well, I would say probably not. I mean, we have prioritized fighting Spam for a long time. We actually have developed in-house technology, and we launched our first version of SpamGuard back in 1999. We have been continually revising it ever since. Consumers' expectation from Yahoo! as an e-mail service provider to provide them a top-notch online experience with e-mail, that hasn't changed and will not change. What has changed is consumers are receiving more Spam today than they were a year ago and two years ago. In fact, we're actually catching five times more Spam today than we were a year ago. So, their expectations continue to be Yahoo!, make sure that you keep my inbox clean and make

sure that you're providing me with an online experience that I can trust.

MR. FRANCOIS: Well, and let me jump back to the study again, which said -- I think it was 48 percent of the people agree that their ISP could do more to stop Spam but is not doing so. Do you find that that is a sentiment that you all have to address and that you've come into contact with on a not insignificant -- insubstantiate basis?

MS. MANN: Well, I very much believe that our customers rely on us to provide them with a top-notch user experience. I would say that our internal statistics actually are a little bit different from the statistics that we've gotten from the Mail Shell survey. In fact, we have done some surveys of our customers, and we say that about two-thirds of our users have actually told us that they are satisfied or more than satisfied with what we're doing to protect them against Spam. I can't speak for the industry as a whole.

I think it does speak to the fact that we are doing what we can and continue to prioritize fighting Spam. Why is that? Because our business relies on providing top-notch, quality consumer experiences, and if we don't do that, then our customers will leave us. So, for Yahoo!, doing what's right for the customer is what's

right for our business, and we're very pleased to hear that we are doing a good job for most of our customers. Is that good enough? Of course not. We always want to try and do better.

MR. FRANCOIS: Just to continue on, you mentioned that your internal study -- and I'd be curious to know what else you all asked your customers about Spam and what their responses were to those questions, not all, but relevant.

MS. MANN: Well, we talk to our customers all the time about all sorts of things, what do they like about Yahoo! mail, what don't they like about Yahoo! mail. We recently did a very small poll on our site to ask our users really a very targeted question, are we doing enough about Spam?

So, the top-line take-away from that is really that two-thirds of them were satisfied, more than satisfied, which is, as I mentioned, comforting to us, but there's still one-third of those people that are not satisfied.

So, that's why it is a corporate priority for us, and we're spending a lot of money and a lot more money today than we were last year and more than a year ago in the fight against Spam.

MR. FRANCOIS: Okay, thanks, Lisa, and I know

that Laura had something to add.

MS. ATKINS: I think one of the struggles that ISPs have to make is they put all this money into filtering technology, but actually determining what's Spam versus what's not Spam is not a technologically easy thing to do, and so they can't ratchet up the Spam filters as much as their users might like, because what I think is Spam and what I don't want, because it's in a Chinese language, for instance, they can't just block all mail in a Chinese language, because some of their customers may actually get mail from people in Mainland China.

And so, the ISPs are spending a lot of money to try and balance their consumer needs with their -- with what the consumer wants, and so Spam filtering is not as simple as it might seem on the surface, because I know what Spam is when I see it, but it's hard to do that automatically.

MR. FRANCOIS: Steve Smith from MindShare Interactive?

MR. SMITH: That's MindShare Design.

MR. FRANCOIS: MindShare Design, I'm sorry, I need to change that name.

MR. SMITH: Bigfoot.

MR. FRANCOIS: Yeah, sorry.

MR. SMITH: I would just observe that I think ISPs are doing what any reasonable business would do, which is just listening to their customers, and as a provider of technology for senders, you know, we have to communicate in recipients' and ISPs' expectations as far as e-mail expectations back to our customers, and we have had to change our definition of Spam from being centered around permission and consent to being basically whatever recipients perceive that they don't want to get, and that's one of the reasons we spend a lot of our time now not just, you know, trying to enforce opt-in and consent, but also working on what are the best practices to make sure that the e-mail that they get is going to be accepted and wanted.

MR. FRANCOIS: Okay. I just want to jump back to -- because Laura mentioned a balancing act, and I know that initially Lisa and I had spoken about some of the things that had to be balanced, and I wondered if you could kind of articulate for us a little bit some of the cost-benefit analysis that Yahoo! has to do in terms of how much to spend on Spam at the expense of other things that maybe they could provide or would like to provide to their customers.

MS. MANN: Sure. As a business that is developing products for consumers, we are always making

trade-offs, of course, given a limited set of resources; however, given that providing for our customers and protecting our customers is paramount for our business, it's not a trade-off for us. It's not an option. We need to invest and we continue to invest in fighting Spam. It's simply -- if we didn't, we would really be risking our customer base, and that's really not an option for us.

So, we do spend a lot of money, and we do spend a lot of time on a number of different fronts, and I can walk through with you the multifaceted approach that we're taking to fighting Spam, and that might give you some sense of the kind of prioritization that we put on fighting Spam at Yahoo!.

MR. FRANCOIS: If you could briefly do it, that would be great.

MS. MANN: Okay, I'll run through it quickly.

MR. FRANCOIS: All right.

MS. MANN: So, the multifaceted approach is really as follows:

We're investing in technology, so we have people at the company that are working on product development, product management, marketing, operations, customer care across the company. We are dedicating human capital to fighting this problem that, of course,

we could be spending on other things, but again, because fighting Spam is such a corporate priority, we have significant numbers of people that are dedicated to doing that.

We have hardware costs and we have machines that are dedicated to fighting Spam, servers that are dedicated to fighting Spam, lots of them. As one of the world's biggest e-mail providers with tens of millions of users, you can only imagine how many machines we have for our system, and there are a lot of those machines that are dedicated to fighting Spam.

A few of the other -- and in terms of R&D and development, we're constantly rolling out features that are helping to give our users more choice in the way they deal with Spam. So, we're investing in -- wow, we need to do things systemwide, but we also need to put tools in the hands of our users so that they can customize and personalize their experience. So, that's really the technology bucket.

The other fronts that we are investing in, and again, making trade-offs throughout our entire business, but prioritizing Spam are on the litigation front, on the legislation front, working with members of Congress to develop effective legislation that is anti-Spam, and also industry collaboration efforts.

MR. FRANCOIS: In terms of consumer complaints, over time, has consumer complaints about Spam -- are consumer complaints about Spam kind of the number one complaint about the e-mail service for Yahoo!?

MS. MANN: It's an interesting question that you ask. Certainly Spam has risen in the public eye. Again, that's why we're all here. But I would say that we are actually doing a better job of fighting Spam today than we have been in the past. One statistic that we have is actually we have seen a 40 percent decline in customer complaints as a result of a new version of our Spam-fighting technology that we rolled out just a month ago.

So, the fact is that while we do hear from our customers that Spam across the industry is an issue, and we hear this from our industry colleagues as well, we know that what we're doing is effective, and we know that every time we roll out new improvements to our system, which we do all the time, each time we do that, we see a reduction in Spam, we see a reduction in complaints.

MR. FRANCOIS: And maybe I can throw this open to all of the ISP providers and anybody else that would care to address it, before I get to Dale Malik, who I have promised to get to and not forgotten about.

To what extent has technology and kind of what

technology is added to make e-mail more consumer friendly and interesting with its features caused more complications with combating Spam? And I'm thinking notably of the ability to use HTML in e-mail, and I've heard from a number of people that, well, that makes it hard, because -- to stop Spam, because a lot of the Spammers try and evade filters by manipulating HTML, and you're getting more HTML graphic Spam instead of text-based Spam.

Mr. Malik?

MR. MALIK: Thank you, Renard.

I think it certainly makes the issue much more complicated from a detection perspective, but I think the customer perspective is even more important, because we have such a large educational gap. You know, most people are on the internet, they love the internet for what it is, but at the same time, they don't necessarily understand the technology like the rest of us do here, and when we deal with customer service issues and folks say, I can see something and it's obviously offensive to me, how come you can't see what I see? And we go through the educational process of saying, well, it's a picture. Only humans can interpret a picture. So, we definitely have both an educational issue as well as a technology issue combined, and that's really what ups the severity

of it.

MR. FRANCOIS: Okay. Anybody else?

MS. MANN: Well, I was going to comment on an example of a feature that we've rolled out recently that has given our customers the ability to deal with those images and those technological problems. It's just an example, but we give our consumers the ability to block HTML images in their messages, and they can go -- they can turn that on simply by clicking on the options page and then checking off don't show me these images. They can also do that from within a message.

So, that's an example of putting some power in the hands of the consumers to be able to deal with these kinds of technological problems that are more difficult for service providers like ourselves to deal with on an entire platform basis.

MR. HUSEMAN: Mr. DiGuido?

MR. DiGUIDO: Yes, we're releasing the findings of a telephone survey today that we've done in coordination with the Roper Organization, and amongst a lot of other things that were asked, they were asked -- the subscribers -- the individuals were asked what they thought the ISPs could provide in terms of help in terms of distinguishing between Spam and messages that they wanted to unsubscribe? And 89.7 percent of them said I

would prefer it if my ISP or e-mail service provider would include an unsubscribe option that would safely remove you from an e-mail list.

So, with AOL, the do not -- you know, the Spam button and all those issues, it's pretty clear that most consumers would want to have their ISPs have the option to unsubscribe out of that mailing and then be able to purge their name from a mailing list, and again, 79 percent of them said that they wanted to see -- and we keep lumping in, you know, volume buyers -- volume senders and pornographers and those folks into the whole -- into the same common definition of Spam. What 79 percent of these folks said was they want to see ISPs treat fraudulent e-mails and pornography in a separate way than they do other mailings that come through.

So, having that unsubscribe option on the same page with your Spam button seems to be one of the solutions that most of the folks that we polled are interested in having from an ISP standpoint.

MR. FRANCOIS: Do you all feel for the service providers a little apprehensive or inhibited about devoting resources to research and development because they may potentially provide the opportunity to be manipulated by Spammers? Mrs. Betterly?

MS. BETTERLY: Well, I have a couple of

comments on a lot of stuff that was said. I'm sorry, I hope you don't mind, but I have a Yahoo! account, and I've had it since 1998, and I've never opted to anything on it, and in the last month I have gotten 11 unsolicited e-mails, which is totally within my tolerance level. So, it's an interesting thing.

On my personal e-mail, though, since it was published on the net and also in the Wall Street Journal, in the last two days, I got 357 unsolicited e-mails, of which 50 were pornography. Now, I'm pointing this out because I understand both ends of the stick here, but the thing that I find interesting and the thing that I'd like to know from the internet service providers is actually how much of this -- these complaints are coming from stuff that has ripped headers, no legitimate unsubscribes and are being hidden, because it's so hard and so expensive for us to be in business legitimately because of all of that? And how many of those complaints are from consumer complaints or actually anti-Spam groups who are actually trying to entrap legitimate marketers? Because you can even see it on the net, they'll actually opt-in to a list to complain. Once they complain, they don't tell you who it is who complained. I could shoot somebody in the street and have more rights.

MR. FRANCOIS: Well, let's defer the law --

MS. BETTERLY: And that's something that needs to be --

MR. FRANCOIS: -- let's not shoot anybody in the street, and at least if we shoot anybody in the street, let's not make it the street in front of this building.

MS. BETTERLY: No, of course not, and I'm sorry, I'm a little passionate about the issue.

MR. FRANCOIS: So, I know Laura is -- Laura Atkins was motioning me to make a comment.

MS. ATKINS: There's a couple thing, and one is what Al said about the ISP should manage the unsubscribe, and I'm not convinced that there's any way they can do that, because the mailers -- a lot of the mailers, particularly the problem mailers -- and listening to you, I wouldn't actually put you in that category, but a lot of the problem mailers --

MS. BETTERLY: Thank you.

MS. ATKINS: -- but a lot of the problem mailers, they don't care. You unsubscribe, and we heard yesterday about how you unsubscribe, and then, you know, two weeks later, you're on -- it's the same company, it's the same whois data, but you're on a different list from them.

So, I'm not sure -- it's -- I understand what

you're saying, but I'm not sure, unless there is a change in the way mail is sent, particularly bulk mail is sent, that does give the ISPs the control over that, it may be helpful, but at this point the ISPs don't have that level of control.

MR. FRANCOIS: Let's go -- Mr. Shivers -- I'm sorry, I don't want to cut you off.

MS. ATKINS: But in terms of what Laura is saying about what people are complaining about, I have a number of clients who -- what I do for them is I manage their relationships with the ISPs, and I manage their abuse box, and I see those unsubscribe requests and I see those Spam cop complaints and I see all of that, and I can tell when my customer has gotten a bad egg on their list, because my complaint rate goes from three or four complaints a day up to maybe 15 or 20, and that's usually based on a single list, and it's a bad customer, and we go and we deal with the customer and it's all taken care of.

So, you know, from the perspective of someone who works with a lot of bulk mailers, if you're getting a lot of complaints, then what you're doing is upsetting your clients and your customers and the people you're sending mail to, and that means you need to change your business, and you need to work to not upset the people

who you are trying to convince to pay you money to sell your product.

MR. FRANCOIS: Mr. Shivers from Aristotle.

MR. SHIVERS: Thank you. We actually do the opposite, and we encourage our customers to not use the unsubscribes, and it's unfortunate. We would love to be able to have that as a valid means for that customer to click and get off that list, but it does not work. We actually go a next step to if your mailbox starts filling up, you've done it once, and then all of a sudden now you're getting 30 a day instead of five a day, we say, okay, what we'll do for you, for free, is you can get an additional e-mail address, we encourage you to put a number in the address so it makes harvesting a little bit harder, and we go to all these links just to prevent the Spam from coming into their mailboxes, and we do also get complaints just daily, just droves.

MR. FRANCOIS: Roughly -- how many customers do you all have? You all are based in Arkansas, Little Rock, right?

MR. SHIVERS: Yeah, Little Rock, Arkansas, which actually I grew up in Houston, Texas. I know that's a good thing to be here, too.

MR. FRANCOIS: I'm a Tennesseean. No, it's not. But roughly how many customers do you all have?

MR. SHIVERS: Appreciate that.

We have roughly 26,000 customers -- it fluctuates. We're a little bit different, because we charge by the hour. In one sense, you could look at it, Spam is -- helps us, because we charge by the hour, but we've also built in systems for our own customers where we have our own browser where they can go in, they get to see the headers, they get to see the subject lines before the mail gets to them, so they can just delete them before they have to pull them, which takes a lot of time.

So, we're trying -- which kind of in a sense cuts our own throat, because then they're not downloading all that e-mail and they're not paying us by the hour, but we have 26,000 customers, and we started out back in '95 -- we're a small business -- we started out with one computer and 32 modems, and Spam now is our number one issue. It's become -- it's shaking the foundations of our business, which is a small business.

MR. FRANCOIS: And we are going to return to that in a second.

Mr. Smith had something to say.

MR. SMITH: Yeah, I just wanted to get back to your question regarding the technology and then some of the capabilities of e-mail, and I just wanted to point out that a lot of the efforts that both mail service

providers and the e-mail client developers are taking to improve the security and reduce the risk of proliferation of Spam in their clients and services is starting to erode some of the fundamental technology in e-mail for like rich media, active X controls, HTML image rendering, and we're at risk -- Spam is putting the richness of e-mails as a medium at risk, and we should consider that also as a factor that Spam is having on e-mail.

MR. FRANCOIS: In terms of the decisions about these features and being able to turn off HTML graphics, I wanted to return to Mr. DiGuido, and we've heard about, you know, Yahoo!'s capability empowering consumers to turn off HTML graphics. Have you heard anything from marketers that say that that inhibits their ability to advertise? Does that -- are they concerned about that in future advertising campaigns?

MR. DiGUIDO: They're concerned, just as Yahoo!'s concerned, in optimizing the relationship between their company and their customers. So, through our technology, we're able to sniff the individual's mailbox and deliver the most optimized message to that consumer that that consumer wants. So, if the consumer says, listen, I want a text e-mail or I'm using AOL and I want an AOL version of the message, we are going to deliver on behalf of that marketer a message in the

context of the way the consumer wants it.

So, through sending multi-part messages, we're basically optimizing the mailbox to the point where if an individual -- like I said, if an individual says, listen, I do not want HTML, I prefer that I receive text messages, then text messages are sent. If they're willing to receive messages from -- that are HTML, they get HTML.

Again, really, where a lot of work is being done on our behalf is working with marketers on establishing that dialogue between the customer. So, driving somebody to a website and saying, I'm now going to start to send you e-mail communications, what type of information would you prefer, and in what format would you prefer it? So, that all goes towards building a tighter dialogue. So, they are not really being hampered at all, because they don't think about it as a broadcast. Everybody gets broad band or everybody gets HTML. They're thinking about optimizing to that consumer's preferences and to their mailbox.

MR. SMITH: Although, Renard, I would respond to that by saying if less people have less capability fundamentally in their e-mail client, that's just going to reduce the effectiveness of the medium in general.

MR. DiGUIDO: That has -- I mean, I take that

point, but again, I think that the power of the medium is really about the messaging and the relevancy to that consumer, okay? I mean, I can't open up a newspaper and have 3D graphics. I can't --

MR. SMITH: Yet.

MR. DiGUIDO: -- each -- well, each medium has -- has been optimized and leveraged for the power that it has. E-mail communication is all about delivering a contextually relevant message to a consumer based upon what they are interested in receiving. So, we've seen some incredibly successful clients using text messaging. You talk about the IT sector or people who are interested in computers, those folks are not traditionally people who are enamored with a lot of HTML whiz-bang type of messages. They want the information in a concise and contextual standpoint, and we've seen incredibly effective campaigns that are text campaigns.

MR. MALIK: I'd just like to add to that a little bit. Some of the experience that we've seen, and I'll challenge the notion that not much has changed from a customer's perspective, I believe that from their relationship with us where two years ago they might have said you're doing an okay job on my behalf as my proxy, essentially, in delivering my mail, now to the point where we have such a wide customer base, people are

feeling, well, you need to help me on my personal level, which is what we're hearing in the conversations, provide me the tools to make my decisions, because this is a relatively complicated technology when we get down to it.

But you now need to simplify it for the customer so that it's -- you know, if I use a telephone analogy like call waiting, you click to get the other call. In the old days, you know, you used to have to -- Molly, please switch me to another line, I hear another call's coming in.

So, they don't understand the technology, so that we need to bring it down to a level that's easy for the customer, give them those tools and I think, you know, some of the discussions here will be very beneficial, agreement on the industry on sort of practices so that we don't kind of bump into each other in the night, that I give you a tool that you inadvertently cut into something that you really wanted.

Because we had a number of customers -- and I am not going to get into statistics now, but some of the internal research that we did, and it was surprising to myself as we looked into it, but there were a number of customers that said I like to look at this, please give me a choice to at least look, because if I am proxying on their behalf and blocking unsolicited mail generically

and I don't give them the opportunity to look at, well, maybe there is something. Maybe there is an offer. It's a -- a thousand shades of gray.

What we had to do is implement -- we actually gave the customer a choice. We said we will completely proxy on your behalf and take it out immediately, and the second option, which we got very good response to, was let me take a look for a little while, and then I'll get rid of it. If I don't look right away, it's time to get rid of it.

So, that's kind of been the negotiation between us and our customer base as we kind of walk towards the -- I'll call it the customer empowerment level that we really need to deal with it generically as an industry and then specifically from each individual customer's needs.

MR. FRANCOIS: Well, let me ask Laura, because I know you speak with many consumers and consumers -- and ISPs about their consumer issues. What are the consumer -- first, what are the consumer issues that they have with Spam? Is it the content? Is it the volume? Is it the fact that it's unsolicited? And what do they want?

MS. ATKINS: Well, the answer to actually all three questions is yes. It's the volume, and it's coming

back from a weekend and finding that you have 150 messages in your mailbox and that two of them are from people you know and 70 of them are mortgage and 20 of them are pornographic, and so it's the volume.

We try and not make it a content-based decision. We believe it is a consent-based decision, and it's whether or not the individual has asked for the mail. You know, if you want to get the porn, hey, go for it. So, we don't believe it's a content-based issue, but what we're hearing from a lot of consumers is that certain content upsets them more, and that contends to be the porn, particularly when you have young children, you know, on the internet, and they're dealing with it, and they're getting all of these porn Spams in their mailboxes, and they're just using a Yahoo! account or they're using a Hotmail account, and when they look on that -- when they click on that e-mail, they get that picture right in front of them.

And I know that there's very little I -- I use the text-based messaging or text-based e-mail program for most of my stuff, so I don't actually see a lot of the images that come through on Spam, but I hear about it a lot, and some of it's very bad.

So, it's the content, but it's also the volume, and trying to delete through things, going through a big

mailbox and trying to delete -- and actually, you occasionally have people who have accidentally deleted mail they wanted because they didn't know or they were going through and they had 15 Spams in a row, and they got to the 16th one, and it was actually a newsletter they asked for or it was actually something they solicited, but they were going through and hitting that delete key, and boom, that's gone, and they've lost mail that they wanted, and that's entirely due to Spam.

MR. FRANCOIS: So, what is it that consumers want? Do they want it stopped? Do they want more empowerment?

MS. ATKINS: I think one of the great things about the internet is it does give the consumer the empowerment to control what is marketed to them, and we're seeing that Spam is trying to bypass that, but there are companies who are doing things that -- to make that channel a more consumer-oriented channel, and they can target it to the individual.

But in many cases, what we're hearing from consumers is we just don't want the Spam. We want the mail we want, and we don't want the Spam, and this puts ISPs in a very difficult decision, and that's why they're spending so much money on research and development, because they're trying to work out what does the consumer

want versus what does the consumer not want, and we are trying to draw that line, and unfortunately for the ISPs, particularly with a huge customer base, is that line can be 15 shades of gray, because this consumer -- while this consumer, okay, they kind of like the porn and they want the porn, and this consumer over here has a bunch of kids and decides, no, I don't want the porn at all, and it's a difficult decision for the ISPs to make, and they're having to invest huge amounts of money into making it.

MR. FRANCOIS: Mr. Shivers?

MR. SHIVERS: First I'd like to say it's a little bit different for a small ISP. I don't have any resources to dedicate to, you know, development. So, what I have to do is I have to go out and get products like -- I mean, everybody knows like BrightMail or Vircom, and I hope to roll out a new one coming up pretty soon this next week is Spam Squelcher. I mean, I have to buy things in a box.

And there's inherent problems in that. What if, you know, one of my state customers doesn't get an amber alert, you know, and am I responsible? I have these worries.

The other thing is, I mean, I just want to read you a little bit -- something from just a customer. I

receive pornography almost every day on my site. It's totally unsolicited. I'm tired of receiving this with the explanation someone has submitted my name and they -- or they wouldn't have sent it. I don't know why we can't stop this, and I spend undue time having to delete it. I have granddaughters who use my computer, and I don't need to worry about the contents of my mail.

And that comes in daily, every system day that we work.

MR. FRANCOIS: So -- and I am not going to neglect the issue of cost, but I am going to segregate that out to a different section that we will explore more fully, but this brings us to kind of the idea of churn and the number of customers that turn over and change ISPs, and one of the questions that I wanted to ask was -- and we will start with Laura, who has some contact with many ISPs -- in terms of the amount of churn in the area and how much of the churn is devoted to -- is because of Spam?

MS. ATKINS: There are some people I have talked to who will tell me that they don't actually believe that any of their customer churn is related to Spam, but there are other companies who certainly believe that they're losing 10, 15 percent of their customer base every few months because of churn.

And what we're seeing -- what I'm seeing in some of the stuff I'm dealing with with my mailing customers and the people who are sending mail is that they can be mailing lists, and as they mail lists, we gradually lose subscribers off those lists because those addresses go dead. So, you know, it's an address that will deliver and will deliver and will deliver and will deliver and then goes away.

From my own perspective and from my own working with consumers, is people don't like to change their e-mail address, because they have given it out, it's on their business cards, their family knows, their friends know, and so it is not a normal choice that they make to change their e-mail address. So, the perception is that some of the churn is absolutely because of Spam.

MR. FRANCOIS: And let me direct this to the ISPs, Dale Malik from BellSouth, I forgot to introduce you, and Lisa Pollock Mann from Yahoo!. I assume that you all both have churn, and one of my questions is, after you all kind of address generally the concept of churn, is are you all gathering -- whatever the percentage of customers that you're losing, which may or may not be attributable to Spam, are you replacing those customers at the same rate, so you're not at a net loss?

For example, if you're losing 20 percent of

your customers every month, are you gaining, then, 15 percent new customers or are you gaining 25 percent new customers? What is the impact on churn with your ISP?

MR. MALIK: Generically speaking, we're still in a fairly good growth market from increasing customer base, and I think churn in the industry is fairly pervasive at this point. I mean, there's been different numbers stated that I've seen in different reports, but basically for us, when we look at the customer satisfaction pieces, is that Spam has been raised as an issue on different surveys of a customer satisfaction piece.

On the good side of the equation, you know, the information we have seen from customers, similar to some other comments earlier, is that the means that we are taking are fairly effective. We're up in the 80 to 90 percent, you know from what we're reading, and this isn't -- there is no statistical way to measure how much you catch, because you can't tell what you didn't catch, you can only tell what you've caught, but when we look out on things like DSL reports and places like that, we see verbatims from customers, and it's probably not statistically valid, but you see things like it's catching 80 to 90 percent, and that is a satisfaction level that says, hey, that's a pretty good job.

But the real issue is as the volume goes up, 80 to 90 percent -- and I'll be ridiculous -- of a million is a lot. So, now, what was a nuisance before is not only just an annoyance, it's almost an invasion of privacy, because it's come into my home, and it's not just resident at my address. People feel that their e-mail address is their -- you know, it's like their personal cell phone. That's mine. That's not just my household's. Now you've invaded my personal privacy. So, it's really now moved to that level, and when you've crossed that boundary, then it's a very important customer service issue and, you know, kind of the round it all up, it can affect churn.

We've considered that, and that's why we make the additional investment to keep it that level, because obviously if you don't do it, then it will absolutely cause churn, because people will say, you know, this is unacceptable. They are not doing enough on my behalf. I will go to somebody who will do something on my behalf. So, it is -- and in certain regards, minimal table stakes. You must do it as a provider. You must do it well to have a good level of customer service, and certainly like many companies in this industry, we pride ourselves on customer service, so it is imperative.

MR. FRANCOIS: Ms. Mann?

MS. MANN: So, our user base, as my colleague on the other side of the table has mentioned, our user base has actually continued to grow. We believe very strongly that that is in part due to the fact that we're doing a good job in fighting Spam.

We are seeing high month-to-month retention rates, and our user base has grown despite the increase in Spam, again, leading us to emphasize why fighting Spam and being good at fighting Spam and providing good user experience is important to our user loyalty.

We also think that's one of the reasons why we've been potentially gaining share over the past couple months, and we have been gaining share. We believe that one of the reasons why is due to the fact that we're doing a better job at fighting Spam than some of the other people out there, so it's very much worth our investment and a very important business decision for us.

MR. FRANCOIS: And Mr. Shivers, as a small ISP, do you have problems with losing customers?

MR. SHIVERS: Yes, well, we're still growing, too. I mean, we put on more customers a week than cancel, but for the first time in the last, I would say six months, we are starting to get cancellations directly attributable to Spam, where before, you know, it's like, hey, I'm moving out of town, blah-blah blah-blah, but now

it's I'm quitting, I can't do this anymore.

It also hurts our branding of our own name --

MR. FRANCOIS: Well -- go ahead, I don't want to interrupt you.

MR. SHIVERS: -- because if you switch providers, let's say you go from Aristotle to WorldLinks, a competing provider in Little Rock, what happens is the nature of the move is they immediately don't get Spam. I mean, because they've moved, and nobody knows where to find them. Of course, they will get harvested at some point in the near future, but until that point happens -- so, what they say is, hey, I moved away from Aristotle, I used to get 30 Spams a day, and now I'm not getting any. You guys need to come over here to WorldLinks and get away from Aristotle, and that's what's starting to hurt our business, I believe, because of the explosion in the last six months.

MR. FRANCOIS: Now, when you said -- at first you said that they were quitting. When you mean -- when you say quitting, do you mean they're stopping the Aristotle service and moving on to another internet service provider or do you find that some people are just quitting to participate in the internet or e-mail?

MR. SHIVERS: Both, I mean both. I have stories here, but I won't read them all, but they are

saying -- and they are just point blank saying, I'm not going to use my e-mail anymore. Well, for us, that means a lot, because that's the primary reason that they're on our business. So, they are quitting using their e-mail.

Also, they are just flat quitting and going to -- well, they go to other places, and we have -- usually, because we cover rural Arkansas, we have a lot of older people who use our service because they're so inexpensive that they are just flat quitting because they can't take it anymore.

MR. FRANCOIS: All right. Ms. Atkins also mentioned the fact that they're finding a number of dead addresses, addresses that are not being used anymore, and I wanted to get Mr. DiGuido and Mr. Smith's input on how that may affect e-mail marketers, the concept of churn and, you know, the fact that maybe you have more dead addresses that are getting -- receiving legitimate e-mail marketing materials.

MR. DiGUIDO: Well, one of the things that happens right away in sending to -- there's all types of things that retention-based, reputable vendors are doing with their own house files in terms of data hygiene and list management in terms of their own lists, so there are services out there that we work with that are ECOA that are looking at helping our clients do a better job in

terms of cleansing their lists of names that are dead addresses.

When we send mail out, we know immediately whether that message has been received to a valid e-mail box or whether it's bounced out of that. So, there's a lot of -- on our side, there's a lot of cleansing of the data and cleansing of those lists, because again, these marketers, they're not in the business of just throwing a lot of stuff up against the wall. They want to make sure that they're dealing with a valid address. So, if we're working with a third-party company where we're doing some acquisition work for a client, we will look at the bounce rate of a given list and take a look at what percentage bounces out of that list, and you're looking for lists with low bounce rates, because those are valid e-mail addresses that are opt-in that people are interested in receiving messages.

So, it's not like in other channels, in the direct marking business, where you could be mailing stuff to a mailbox and it's being delivered but there's nobody home. Here we know immediately whether that message has been received by a valid e-mail address or not, and the next step is we know whether people opened it or clicked on it. So, that level of reporting is something that you don't get in any other media.

MR. FRANCOIS: Mr. Smith?

MR. SMITH: Yeah, I would echo Al's sentiments, and a lot of that, I think that there's some very basic list management and data hygiene and list hygiene techniques that responsible mailers employ, you know, taking your bounces, interpreting the bounce codes appropriately, removing the hard bounces off the list, dealing with soft bounces appropriately, and I think most -- most of the legitimate services, like Al's and myself's, that do these types of things do these basic functions as well as provide the reporting, click-through, open tracking, so that you can actually try to limit your list to the people who are getting it, who are opening it, who are responding to it and get rid of not just the invalid addresses but the inactive people as well, the people for whom the messages aren't relevant.

MR. DiGUIDO: Those marketers are taking -- I don't know, Steve, you might see this, you probably do, the whole ROI factor, using e-mail as a cost-effective and efficient way to get out to an audience, it's only effective if the message is delivered to most mailboxes, a certain percentage of the folks open them and actually take some action.

So, the level of accountability in terms of the

performance of this medium, I've never been involved in any other medium that is as accountable in terms of return on investment amongst reputable vendors as this one has been, because all the capability and the technology and the reporting is all there to provide that level of accountability.

MR. FRANCOIS: Yeah, absolutely.

Mr. Lewis from NortelNetworks?

MR. LEWIS: Yeah, I'm coming -- we're coming from a somewhat different perspective than the ISPs and the marketers. Being a corporation, we have a somewhat different perspective on how we use the internet. One of the comments I'd like to make about some of the issues that have been discussed is that they were mentioning about reputable marketers and bounces.

One of the things that we have been discovering is that a lot of the even big name marketers that you would assume and usually are quite legitimate, some of their bounce handling is quite bad, in addition to the more obnoxious and more deceptive practices who couldn't receive a bounce even if you did bounce it, but we have had a number of issues with major marketers not being able to do very good bounce handling.

For example, as I mentioned yesterday, one of our old domains we turned off for a period of over a

year, and the day we turned it off, we were getting 50,000 e-mails a day to it, and when we turned it back on again a year later, we were getting 600,000. And during that year, every single piece of e-mail to those addresses bounced. So, obviously bounce handling is not handled in a very -- very well in a global fashion.

The other one I wanted to mention was the issue about inline images sometimes where they were talking about open-up, you know, you can tell that your recipient opened up the e-mail message. As many companies, particularly major ones in the internet, we're also very concerned about our own security, and things like knowing when our user opens up a piece of e-mail is something that we do start to look upon as being a security issue, and there are many other things like that.

For example, we have been balancing the options about inline images, like the one pixel, did this person preview the e-mail, and we've been trying to balance, should we block those or should we eviscerate those? And the first thing that we think about is, who's the biggest person who's -- who's the most prominent person that we see doing that? And it's EVA (phonetic) groups. And we certainly don't want to interfere with that.

On the other hand, we have things that are saying, well, most of the major browsers on the internet

or that are used on the internet, just by having that subject line headlighted or highlighted, you have an HTML request going back to the sender that not only tells you that the user has seen your message in some notion of seeing, but what it also can be used for is a form of being able to say, well, the user confirmed because they clicked on something, the browser did it for them. And in fact, from what I understand, the current versions of Netscape do not have the ability to turn that off, and the next version does. So, we have some issues surrounding inline active content.

For both anti-Spam issues and for anti-virus issues, we have had to deliberately start banning certain kinds of content -- sorry about that -- and I think that some of the marketers will start to find that the -- most of the media, the rich media they are trying to use is being blocked not only from an anti-Spam perspective but from an anti-virus perspective. Most people who are power users will have noticed that it's starting to get very hard to send executable programs anywhere. Well, it's going to get that way and much worse with even simple things like HTML and inline images.

MR. FRANCOIS: Now I am going to jump back to Mr. Malik for one last comment before we actually return

to Mr. Lewis to talk about the impact on businesses as well.

MR. MALIK: Some of the discussion has been around what I'll call dead accounts. There's also another element that needs to be considered as part of the cost as we get into this, it's really abandoned accounts. We have a number of customers that -- maybe their initial account that they have had for three years is now no longer usable from their perspective, and some of the suggestions were made earlier, we make to our customers, you know, moving to a slightly different account name, adding numerical things. There's a bunch of different suggestions depending on the situation the customer is in, but that's when we have knowledge that the customer is moving, we can take action to maybe remove the -- I don't know, the abandoned or moved-from account.

But when you have -- and I'll use a -- probably not the best analogy, but when you have abandonment of a sort, you can wind up with effectively ghost towns in different sections of your systems that people that have been maybe long-standing customers have had to go get other accounts because they have no way off of these lists. They have no way to really drop this down. And they have other accounts they can go to.

But now, from a provider's perspective, I need to carry the cost and the maintenance for those abandoned accounts, and they continue to get mail, because not everybody is doing the policing of their accounts to see if somebody is up. They really don't care. They just know that it went out, it's still a valid address, they are going to continue to pump mail at it, continue to, you know, have me hold storage for some period of time. So, that creates this other secondary effect that, you know, really isn't that well known in the industry, and it's perfectly fine for the customer to move and it's a good thing to do, but I can't tell that they've moved and stop using it quite as easily as if they come and tell me. So, it creates another issue.

MR. FRANCOIS: And some of the people that I have been -- okay, some of the people that I've spoken to have said that as a way to control the amount of unsolicited e-mail that they receive, they have several e-mail accounts.

MR. MALIK: Correct.

MR. FRANCOIS: Devoted to specific purposes, and some are devoted just to simply sign up for something and catch the unsolicited e-mail, and they don't really use it for anything else, but it sounds like you're saying that can have a pretty -- still cost you.

MR. MALIK: Exactly, and it is -- and the interesting thing is is that the customer feels that it's not usable anymore and it requires no maintenance by them, which is a reasonable expectation.

Now, in a -- kind of a back-end operation side, we have to go look and see how many of those accounts maybe haven't been used in, I don't know, pick a time period, six months, and have they filled to the brim with e-mail, and if you take a quick look without looking at the contents, there's, you know, maybe -- I'll make it up, a thousand messages all between 7 and 10K, which is about the size of a normal Spam message. You can reasonably assume that that's what's in there and it's just been flooded with that and now you have got to start going with your maintenance issues or cleaning that out.

So, it is a -- you know, if you want to call it public works maintenance, it's a form of that, but it is definitely a side effect of the volume that's gone up, and more and more people are feeling forced to abandon accounts because of that, because of the volume that's increasing. Say, I just can't take it anymore, I am going to move over here. So, that's why the issue is moved to that space.

MR. FRANCOIS: Okay. We have talked about -- it looks like you wanted to say something.

MR. DiGUIDO: Well, what I would say is I think that the -- there's no doubt that the consumer, if you gave the -- an option to the consumer on a free service to have a mailbox that was secure delivery, something that they could say, okay, on that mailbox, the things that I want and I've told you that I want can be delivered there, that would be a great thing for the consumer, and the marketer -- I mean, the impact to the reputable marketer in terms of Spam is significant. It's clutter. It gets in the way of their permission-based e-mail communication getting to the customer. So, the marketers would embrace that type of an effort as well.

The big, big issue that I think that we have to address as well is that -- as we talk about Spam, and Laura has mentioned this before, this delineation between what is Spam and what isn't, we -- the poll that we did, 40 percent of the folks that responded said that they -- that a message that they wanted, they wanted to receive from a reputable, trusted source, didn't get to them, and when you're dealing with companies like ourselves that work with a lot of financial services organizations, that are starting to use e-mail for service messages, and a service message gets caught up in a Spam filter and I've suppressed direct mail, now I don't get my billing statement.

Well, that's a significant problem. So, there -- you know, as much as we hear the stories about pornography, we want to put that over on the side here, and fortunately it's over on the side there, but we don't want to use the same brush to kind of sweep away the stuff that needs to get there from a consumer standpoint. So, a separate, secure mailbox or given an option for that would be something that I think marketers and consumers would be interested in.

MR. FRANCOIS: We've talked about marketers, consumers, and we want to talk about the impact on unsolicited commercial e-mail on businesses and what that does, and for this we are going to turn again to Chris Lewis from NortelNetworks, and I know that they have undertaken some efforts to actually quantify how much it costs their business for each Spam that gets through their system. So, we'll --

MR. LEWIS: Yeah, we have been able to quantify parts of it. I think it's important to mention a little bit about who we are, because we have a sort of an unusual position in terms of the internet being -- NortelNetworks is one of the world's largest manufacturers of internet equipment. A lot of the wires and equipment that your e-mail travels over is produced by Nortel or its various competitors. So, we are very

heavily reliant on the internet both as we build it, but also because we do business over it, because that's how -- that's our whole -- that's our business, in addition to the telecommunications industry and telephony and so on. So, we rely on the internet to do business.

Logically, if you look at this at a high level, you'd think that a company like NortelNetworks would benefit from Spam, because it's increased bandwidth, more hardware, more equipment, but it's not working that way. We find that instead that Spam is having a chilling effect on the industry as a whole. People have alluded to stories about people who have abandoned the internet completely.

Now, of course, you know, everyone knows the internet is having various economic difficulties, and I personally believe that much -- some of what we are seeing is actually because of this chilling effect. Of course, there are other issues involved about over-capacity and so on, but what we're seeing is that it is driving some consumers away, and it's inhibiting the growth of the internet. That's what's inhibiting our bottom line, is the growth of the internet itself.

One of the best ways of looking at that is that there have been a number of studies over the years in the UK and in the United States about lost opportunity costs

due to Spam, on the order of billions of dollars.

We're very much unlike an ISP in some ways and like an ISP in others. E-mail to us is a mission critical resource. We use this to do business. That's how we do our deals. That's how we support our customers who are buying our equipment and so on. But we also give our users considerable latitude in what they can do on their own, what they can do for a personal basis.

So, while our employee agreements will prohibit certain kinds of behavior, which we'll touch on a little bit later, we do allow people to buy things using their NortelNetworks connectivity and so on. So, that is sort of our, you know, introduction to it.

We have some advantages over an ISP in dealing with Spam, because there are certain things I can look at and say, yeah, that's Spam, that's blocked -- that gets blocked, and our users, who are employees, don't get a choice.

Now, there are a lot of other things where the converse of that is that a -- the consequences of accidentally blocking something we shouldn't is considerably -- can be considerably higher, because when you're talking about very, very large contracts about selling equipment around the world, a missed piece of e-mail can delay something or can lose a potential sale

all altogether.

So, we have a very difficult balancing act about, yes, certain classes of Spam are easier to determine and block, but on the other hand, our false positive rates of accidentally misidentifying something as Spam, the consequences can be considerably higher.

And the other thing that it would be interesting, is very worth pointing out, is that we have very little churn with employees due to Spam, because how many people are going to quit their job because they're getting too much Spam? That's obvious. On the other hand, if you're not doing a very good job at Spam control, you can have a serious impact on your employees.

So, I'm going to give a little bit of our numbers here just to give you an idea of the scale of the issue we're dealing with, and I personally believe that we're -- the industry, the e-mail industry, is actually in serious trouble right now. I'm in a unique position that I have been involved with e-mail -- with Spam in various forms for almost a decade, but we are seeing this exponential growth, and it is getting truly, truly frightening, even over the last couple of weeks, the numbers are getting staggering.

When I first started with e-mail Spam, we're talking about less than a 1 percent, a few thousand

e-mails to a user base of 50,000 to 60,000. Nowadays, I did some -- I ran some metrics about a month ago, and between 75 and 80 percent of all of our inbound e-mail is unsolicited bulk e-mail. That's over 1 million Spams each and every day. And it's now doubling every four to five months.

Now, I say that, that's the sort of accepted value, what BrightMail is talking about. The thing that really scares me is I'm looking at numbers over the last two weeks, and I am even afraid to quote because people are not going to believe me, but over the last six weeks, we were seeing doubling on the order of every four to six weeks. It's just totally unbelievable.

In a few months or even a few weeks, we're going to be seeing 2 million Spams a day. We are going to be seeing 4 million Spams a day. Many of our employees are getting -- routinely getting a hundred or more Spams per day. These are real numbers of stuff that they report to us or stuff that we have blocked from them. We're somewhat different than other ISPs and some of the industry where we have direct channels to our employees. We tell them how to behave when they get Spam, and we tell our users, do not click on the Spam -- do not try to do a delete.

We believe that in many -- in most cases,

certainly with many of the legitimate marketers represented here, if you go to their unsubscribe and you hit unsubscribe, you will get unsubscribed. We have no problem with that, with believing that, but a lot of the stuff is not that way, and when you see some of the studies, like the CBT study, they talk about, well, we tried four or five e-mail addresses, we seeded them in a couple places, and then we unsubscribed, and we didn't see those addresses getting more Spam. Well, that sample size was simply not big enough.

We have 50,000 users. We see a different behavior. What they talked about, if this e-mail address disappears -- if -- once this e-mail address was Spammed the first few times, if you didn't seed it somehow, the volume tailed off. Well, that doesn't happen. We are seeing a jump from 50,000 to 600,000 over a one-year period where the mail was 100 percent undeliverable.

MR. FRANCOIS: So, Chris, let me interrupt you. What are the steps that you all are taking to --

MR. LEWIS: Well, I was just going to -- okay, yeah. So, you wanted to talk about steps.

MR. FRANCOIS: Well, no, I remembered we were talking and you gave me in terms of the study that you all had done and what you all had figured out in terms of

how much it cost you all in terms of lost productivity.

MR. LEWIS: Okay. In addition to the various costs like bandwidth, increased bandwidth -- I mean, when we're talking about 80 percent Spam, 80 percent of our bandwidth costs are due to e-mail or due to Spam in additional equipment. We have dedicated anti-Spam servers. We have people who are responsible for operating these things and for tuning them and so on, in addition to all of the other effects about reputation lost due to people forging in your name.

I decided to take a very focused approach on trying to justify doing anti-Spam at NortelNetworks, because when this thing first came out, when I first started working in this area and start dealing seriously with e-mail Spam in '97, there wasn't very much Spam, and nobody thought it was a problem, but I thought it's going to go like this (indicating). So, the focus of our -- of the study that we used to justify our anti-Spam work is how much productivity is lost for every e-mail Spam that gets through to the end user?

And the number that we're using right now is that every Spam that gets past our filters to one of our users costs us about a minute of lost productivity, and that would seem surprisingly high. I mean, the Spammers will say, well, how long did it take to just hit delete?

Three or four seconds to -- I have to recognize, oh, yes, that subject doesn't look kosher quick enough, but what those aren't including are things like how long does it take to download that message to your thing. That's, you know, relatively straightforward technological thing. But what we have is a much bigger issue around most Spams do take 10, 15, 20 seconds to just purge out of your way, but there are many Spams that take considerably longer than that.

For example, we have Spams that trigger security investigations. I just got a pornographic Spam from my deskmate. How is he allowed to do this? And then we have to figure out, oh, no, it didn't come from our deskmate. The Spammer forged this address. Or the types of content or senior management finding -- trying -- yelling, how did this person find out my e-mail address?

So -- and then it goes into Spams that subvert browsers and put out pop-ups and pop-unders and trying to kill things. Many of us have seen Spams which will open up multiple windows, and when you start closing them, new ones will pop up. How long does that take to deal with? We have -- especially with some of the more objectionable material, Nortel is in a number of different places around the world where certain things

are even more objectionable than they are here, and we're dealing with employees who will get something that literally puts them off their work for 10-15 minutes, an hour or days.

We have had situations where people call you literally in tears about the material they're getting, and that means we lose the benefit of our employees for that period of time. That also involves complaints up and down the management chain whenever a senior manager gets Spammed, support costs for complaints and employees trying to, in addition to our Spam filters, put in their own Spam solution problems. So, I said that that takes about a minute of each of our employees' time.

Using our loaded labor rates, which are relatively in line with the rest of the industry, and rounding up and rounding down and so on, we are basically looking at every e-mail that gets past our filters costs us $1 in lost productivity.

MR. FRANCOIS: And roughly how much e-mail gets through your filters on a daily basis?

MR. LEWIS: On a daily basis, we are estimating between 5,000 and 10,000 are getting past our filters.

MR. FRANCOIS: So, according to your study, approximately $5,000 to $10,000 a day --

MR. LEWIS: That's right.

MR. FRANCOIS: -- in lost productivity.

MR. LEWIS: Now, if our filters weren't as good as they are, we would be talking a million per day. So -- and it's taken six years to keep the effectiveness rate that we have, and we have played a number of tricks that aren't available to ISPs to try and make our filtering job easier, but I really can't go into those.

MR. FRANCOIS: I know Mr. DiGuido had something to say.

MR. DiGUIDO: Yeah, I'm just sitting here listening to this, and I've been watching this debate played out on major periodicals in the country, and the words that are being used are just incredible, chilling effect, that the e-mail industry is in major difficulty and that the scourge of Spam -- I'm not trying to denigrate the debate or the conversation, but we need to put it in proper perspective.

The e-mail industry is not, from a reputable marketer's standpoint, in difficulty. More marketers today are spending more time on just trying to understand the e-mail delivery channel than ever before. We are being inundated with major companies who are looking at this channel of distribution as a way in which they can communicate to their customer.

The scourge has been the cost of other media in

terms of delivering an audience from a prospective -- whether it's an acquisition message or attention message. The cost of paper, printing and postage, continue to go up. The cost of all media continue to go up. Marketers are faced with incredible challenges today in terms of instilling vitality and triggering the economic conditions of their company. E-mail has become a place that they have found as a refuge amongst all of those different issues.

So, I take great cause in terms of the whole issue that the e-mail industry or the internet industry is in serious difficulty. What needs to change, and we're not talking about that here, is the economic relationship between the ISPs, the providers like ourselves, and the marketers, the reputable marketers. That's what needs to change. If the ISPs had a piece of this overall transaction, this relationship, we would start to see commercial service. We would start to see dedicated places where consumers could go for minute messages that they would be willing to pay for to receive.

So, I think that any opinion or any statement that comes out of here that says that the e-mail communications business, that the internet industry is somehow in dire straits, I mean, after all of what's

happened in the last three to five years, I mean, business models have failed, no doubt, but this delivery channel continues to grow. Reputable marketers continue to work with reputable firms to figure out the secret sauce, the way in which they can communicate in the customer's preferred channel, which happens to be internet, in an effective -- cost-effective and efficient way.

So, if it's up to the NortelNetworks, the BellSouths and those folks to figure out a way or the Yahoo!s to figure out a way that commercially this makes sense, then let's have a conversation about that, but to say that the industry is in difficulty, it's not.

MR. FRANCOIS: And let's turn to Ms. Mann, who has a comment.

MS. MANN: I just wanted to add that from our point of view, e-mail continues to grow as well, so yes, Spam is becoming an increasing problem. We hear from our customers, we see it, we all see it in this room, but e-mail usage around the world continues to increase. The number of people who are using e-mail continues to increase. The number of people who are transacting online from our point of view at Yahoo! continues to increase. So, certainly online activity is not being squashed by Spam.

But of course, it is a priority to continue fighting that, and we do need to work with lots of players in the industry, with people who are doing direct marketing with legitimate marketers, with people who are working from the corporate perspective, with people who are working to protect consumers like we are, absolutely. So, I just wanted to echo that sentiment from our point of view, as well. Despite the fact that fighting Spam is one of our top corporate priorities, we do see the continued growth of e-mail users and usage.

MR. FRANCOIS: Okay, let's turn to Mr. Malik, he has a comment.

MR. MALIK: Thank you, Renard.

Even though, you know, we're certainly not in any state of a crisis, what's really a business concern I think to any business that would be trying to baseline costs or, you know, forecast revenues and profitability, this issue, because at least in the last six to eight months, as the amount of Spam has increased and become more the predominant volume of mail in our systems, whether we're taking it out or not, it's still there, and there's a cost to take it out.

So, if some of the figures that we've heard from some of the other panelists continue to grow, then from a cost to your business perspective, if I'm going to

provide let's say some new advanced e-mail service to businesses, today that cost is one number. If I can't forecast the future six months, 12 months, whatever that horizon is that I'm preparing a business case for for investment, it makes it very, very hard to run the business going forward, because I don't know what my cost base is going to be, at least that I can control.

So, this creates another element that I don't have direct control over, even though I'm controlling customer satisfaction, but my actual internal costs now have a variable that is unknown.

MR. FRANCOIS: Let's go to Mr. Smith and then Mrs. Betterly.

MR. SMITH: I just wanted to expand on what Al said regarding e-mail and echo the sentiment that, you know, our business is growing quarter over quarter in terms of revenue as well, so it's not a -- it's not all doom and gloom, although we do realize that spam probably is the biggest threat to e-mail as a medium, but if you take a step back and look at e-mail as a medium or a communication method, it's still relatively young, you know, 15-20 years old compared to television, radio, newspapers, the telephone, all these other communication methods and mediums have been around a long time and have had a lot of -- a lot more time to work out the kinks,

if you will.

MR. FRANCOIS: Mrs. Betterly, briefly.

MS. BETTERLY: Well, I see it as profitable, and it is profitable. In fact, you know, coming from the dot com world, it was more profitable than having a dot com with 150 employees, you know, with nine people, we actually draw profit and we do well.

MR. FRANCOIS: And why is that?

MS. BETTERLY: Well, I mean, first of all, we're not -- we absolutely refuse to take any investors, so we make more money than we spend. We have to -- you know, we have to be -- we have to actually look at the bottom line and look at what we're spending and whatnot and what's getting through and what's not. So, there's a lot more control on the finance itself than there was, you know, several years ago when, you know, you could spend $30,000 on a party, you know, that doesn't happen anymore, you know, we spend $20 for dinner, and it's, you know, those kind of things.

So, I see it as one of the few profitable things that you can actually do on the internet as opposed to some of these other models that looked really good that are no longer there, that were cool technology and whatnot, but at the end of the day, there was no -- there was no revenue model behind it. There is a revenue

model behind what we do.

And at least, I'll speak for myself, trying to do the best we can to be as legitimate e-mail marketers is that we're very interested in getting rid of the guys that are overseas and ripping headers and sending out things that are absolutely -- it's affecting me economically. It's harder for me to actually do my job, even though I get virtually no complaints. You know, I get filtered out, and I know I can see a big difference in the response rate. I mean, in fact, sometimes we don't even send to AOL anymore, because -- I mean, even though we don't get any complaints, they look at our stuff and say it's too many, and we -- so, you know, there's that.

We also have to make sure that the names that we have, that we have enough information about each individual -- the original lists that I was working with didn't have time, date, IP and physical address. I don't send to anyone who doesn't have that anymore, because I have to show exactly where this guy came from in case I get a complaint.

MR. FRANCOIS: And I hate to cut you off, but we are going to move to Mr. Malik and talk a little bit more about at least the costs and the impact of Spam and the growth of Spam that he's seen at BellSouth.

MR. MALIK: Thank you, Renard.

Over the last three years or so, I'm going to try to paint the picture from 2000 to 2003, and give you an idea of the juxtaposition in time and perception, and if I look at the year 2000, you know, we're looking at Spam as being, you know, from a customer's perspective, I'll call it a minor nuisance, and in the single digits within our systems. So, from our customers looking at it and our cost perspective, we are spending adequate money to deal with the problem at the level that it was at the particular time.

The main focus of most of our work was really strictly on more abuse and just general Spam filtering. We weren't to the personal level that we talked about a moment ago that's now -- because it's moved into the space where in 2003, we're looking at in excess of 70 percent of the mail that we handle is Spam. The ones that we can see, where we have seen a dramatic increase, in just -- I think someone else mentioned on the panel, just the last 60 days, we've managed to see an increase from near 48 percent that we are seeing to over 60 percent, in the mid-sixties. That's a 25 percent increase in things that we're seeing.

So, if the average person is, you know, has a filter rate that's let's say 15 to 20 percent is still

getting through, that person is seeing somewhere around 70 percent coming towards them, and then, of course, you know, a portion of that is passed on that we are not able to catch. So, that is a significant cost to our business, because if you look at the total volume of mail and consider that 70 percent -- 75 percent of our inbound traffic is Spam and 25 percent is not, if I assume a one-for-one inbound to outbound -- close, let's not get into a long discussion about it -- then that means that 60 percent of my capacity carrying cost is attributable to Spam today.

If I go back to 2000 and I do the same math, the numbers are dramatically smaller. Basically what it's caused is almost about a 5 to 700 percent increase in our day-to-day carrying costs to carry Spam.

MR. FRANCOIS: And that's over what time frame?

MR. MALIK: That's over a three-year period.

MR. FRANCOIS: That's over a three-year period?

MR. MALIK: Not quite three years, you know, I'm not -- we didn't time stamp 2000, and we're here early in 2003, but over that horizon.

MR. FRANCOIS: So, over the past few years, basically a 5 to 700 percent increase?

MR. MALIK: Right, and then the big, steep curve has really occurred in the last year. I would say

that in the last year -- and I can't tell you what the stimulus is, why it's happening. I think part of it has to do with the fact that as our technology as providers has gotten better, we'll use math, if I still want to get ten messages through, the way to get ten messages through is as the filter gets better, I up the volume, and I still get ten messages through because my goal is to get ten messages through.

So, that I think is one of the reasons that we're such a higher volume as we've gotten better with the technology. So, you know, as we get good, we also have to take the burden of responsibility that we're also going to have to deal with more until we change some of the behaviors or the way we're dealing with things.

So, if this continues along this rate, and I hope it doesn't, you know, we could be seeing, you know, somewhere close to 80 percent in the next couple of months, which would basically be such a significant amount of cost in my system that for every customer that I take on, I'm going to be looking at somewhere between $3 to $5 a year per customer to deal with Spam alone, which was not in existence a couple of years ago, not to that level of magnitude, where it was really a cost consideration and a business case, that we have got to invest -- I think some of the things that I've heard to,

you know, in the technology, the people and so forth to deal with it. So, it's a real cost to the business from that perspective.

MR. FRANCOIS: Before we get to Mr. Shivers, I want to ask Dale, what is the most significant cost that you have? Is it hardware, software, abuse desk?

MR. MALIK: I'd say the most significant cost is at the system level and the software that we have to run, because if you're thinking that 60 to 70 percent of my systems are tied up doing Spam -- processing Spam, and I have a fairly significant investment in those systems, because that is the next largest system, mail, besides our internet access, that's a fairly good portion of my cost base.

MR. FRANCOIS: Okay. Mr. Shivers?

MR. SHIVERS: Back in -- it was just not that long ago, it was like February of 2002, we were running 35 percent of our e-mail was Spam, and now, right now, we're running 65 to 70 percent of our e-mail is Spam.

MR. FRANCOIS: Is that e-mail that's coming into your system, e-mail that gets through to the --

MR. SHIVERS: No, that's e-mail that's coming into our system. If you look at 4 million messages, approximately 2.5 million would be Spam, 1.5 million would be supposedly good mail, but you have got to --

you always have to remember, like Dale said, that 15 to 20 percent of the stuff that is getting through is also going to be Spam, and that's been -- since Spam is growing exponentially, that 15 to 20 percent, where two years ago it represented a very minor nuisance, is now becoming an overwhelming situation.

From my standpoint, it's not just the customer complaints, it's not just the systems I have to put in place. I'm at the level of about $5 per customer per year, what I'm throwing at it, and for me that's a lot.

MR. FRANCOIS: And you earlier alluded to the fact that you all charge per time.

MR. SHIVERS: Correct.

MR. FRANCOIS: And so that has -- I mean --

MR. SHIVERS: Our average customer is about -- they spend with us about $6 a month, so if you figure $5 a year, that's quite a bit per customer.

The other side of the coin is right now, I am actually behind the curve. I am not -- I don't have the resources to keep throwing -- I mean, I am throwing -- I will throw as many servers as I have to at the problem, but I am behind the curve. So, to me, to survive, I'm doing everything I can, but it's almost like every day I'm fighting a denial of service attack.

Just to give you a little story, I left to come

down here, I got up at 4:00 the morning on Wednesday to, you know, get on the plane to get an early flight down here so I could see the afternoon sessions. The first thing I did when I got up and went and got into my computer to see how my connections were doing, to see -- and I was amazed. It was 4:00 in the morning, and each of my servers had 500 connections, and I have three filtering services, and they had 500 connections apiece to it. And they don't function too well over, like, 400. So, I was being hurt at 4:00 in the morning.

The last thing I did before I stepped out of the house to get on -- to go to get on the plane was to check that again. As soon as I got to Charlotte, I called my engineer and said, hey, what's going on? And he had to call our vendor to see what was going on. Then, luckily, I was at the open relays and proxies thing yesterday, came up with a good idea. I called my engineer immediately -- I walked out of the room, called him, said get on that list right now. So, that's what we're fighting.

MR. FRANCOIS: What are -- I know you alluded to not having the resources, but what do you find as a small ISP that because of limited resources you are not able to get to try and handle this situation? Is it a better filtering service? Is it more servers? Is it --

what is it?

MR. SHIVERS: Well, it's two things. One is it's -- yeah, we're -- I'm not touting this new technology, but we're excited if it works. I think it will start helping us. It's one that actually will punish, so to speak, the Spammers hitting our system, because it will actually tighten down on their bandwidth and then allow the good mail to come through. We're hoping that that works.

The other side of the coin is when we get into these positions where it's almost like a denial of service situation where our servers start delaying mail, our customer complaints go up astronomically. Our customer support team struggles to keep up. Our customer service team struggles to keep up. Our switchboards light up. It's just -- that's where we go.

MR. FRANCOIS: And roughly how many employees do you have that spend -- how many do you have, and how many of those spend the vast majority of their time dealing with Spam issues?

MR. SHIVERS: Well, customer service and customer support combined, we have seven people that do those, those aspect of our business. Right now, just to monitor systems, that's part of my job and my network engineer's. So, we basically have two that are

dedicated. He covers DSL, and I cover other issues, like we also host websites, like most small ISPs do and we have domains and all that, but it used to be that's where I would spend most of time and getting new servers and taking care of that or our website design teams, but now I'm spending about 25 to 30 percent of my time dedicated to this issue alone, and he's spending probably 50 percent. So, our other aspects of our business are starting to suffer.

MR. FRANCOIS: How much yearly, if it's possible, do you all spend on addressing Spam issues?

MR. SHIVERS: Well, today -- well, we started in about April 2001 with the Brightmail folks, and to date, we've spent something in the neighborhood of like $112,000, and I anticipate, just over the next six months, I'll probably have to like spend that type of money again just to keep up with the problem.

MR. FRANCOIS: Okay. And I want to return to Dale for a brief moment in terms of the increase in costs you said over the past few years has gone up anywhere between 500 to 700 percent, and my question to you is, where does that money come from? Does it just eat into your profit margin? Do you increase your monthly access fees? How have you all tried to address such an exponential increase?

MR. MALIK: Right. So far, it's really been built into the base cost of running the business. You know, I don't believe our pricing has changed much over the years. In fact, the pricing pressures, many are aware in the industry, is the other way, coming down as, you know, as competition is fairly fierce in the marketplace. So, it really does -- it raises our general cost base, which at some point, you know, the consumer is paying for it depending on how you look at it.

But of course, because it's in the expectation level now that this is something you have to do on my behalf, and you must do a good job if you would like my business, then, of course, it has to be incorporated into the bottom line. There isn't -- you can't separate it out.

MR. FRANCOIS: And you know, there's a lot to cover on this, but I want to kind of talk about something that we had briefly or I had e-mailed to everybody is with the onslaught of proposed legislation, we wanted to kind of address some of the economic issues and, you know, keeping in mind that there will be a state and Federal legislation panel that will address these issues -- more issues in more detail, I sent you all a link to the Burns-Wyden legislation that was introduced and

wanted to get your opinions, brief opinions, because we're running into our question and answer time period, on whether, if this legislation is passed, whether this would have any effect on your economic interests, whether -- good or bad, and what would it bad.

Actually, I am going to start with Steve, who will talk about that briefly and also potential -- the impact of the tapestry of state laws that are out there.

MR. SMITH: Okay, so, as far as Burns-Wyden, the two main areas where we see that potentially impacting our business economically is, one, in our exposure to litigation and frivolous lawsuits, and two, on whether or not it actually does impact Spam or is able to control Spam.

First, in terms of litigation or frivolous lawsuit exposure, the existing -- you know, the existing state Spam statutes that are already out there, I think it's 27 states have -- and somebody can correct me if I'm wrong -- 27 states already have state laws in place regulating Spam, and some of those laws are relatively poorly crafted, particularly like in Utah, for example, there's a great exposure to frivolous lawsuits, and we actually were named as -- one of our customers was in a lawsuit where we found that -- in our research that the recipient in question who received the e-mail, there was

records showing that they actually did subscribe when it came down to it, which is kind of scary, because it kind of shows the potential for abuse of a poor law.

MR. FRANCOIS: Do you know roughly how much it cost you to litigate and research that issue?

MR. SMITH: That particular one I don't have the numbers on, but it's thousands of dollars generally, and every time that happens, you know, you can't just ignore it. You have to actually respond to it.

And, in fact, there was an article two days ago in DM News quoting Al Mancell (phonetic), the president of the Utah Senate, and Martin Stevens, Speaker of the Utah House. They are trying to pass some amendments to correct that law, and they said that Utah's current law, and I quote, "has resulted in the proliferation of over 1500 lawsuits in the last ten months. Two Utah law firms are taking unfair advantage of our legal system." And that's from Utah legislators.

This is one of the reasons why we think Burns-Wyden may actually be a benefit to us if we can get one consistent well-crafted Federal law rather than potentially 50 different state laws all regulating things in potentially conflicting ways. I think some of the laws, if you look at them now, actually are conflicting in the way they address this. And I think also if you

consider it, it really doesn't make sense to have state-level legislation addressing a global network.

MR. FRANCOIS: And I'm going to move on to Mr. Shivers, Burns-Wyden and your economic interest.

MR. SHIVERS: Well, I don't think it goes far enough at this point. I think there's some definitions that need to be added in there, because it would -- that has to do with the sender. If it's -- there needs to be like a right of action in relation to both company and e-mail sender, because otherwise, companies can just move off-shore, and what's our recourse? And there won't be very much.

MR. FRANCOIS: Is that because of the -- the problem lies in the volume that you receive?

MR. SHIVERS: Yes, I would say so.

MR. FRANCOIS: Okay. Mr. Malik?

MR. MALIK: Well, generally speaking, any legislation that is going to hopefully take some of the Spam out of our network, you know, through legal means will certainly be a help and, you know, as we're looking at this bill and other things that are out there, we plan to spend, you know, a reasonable amount of time providing input into some of these complexities, because I think as many of the panelists agree, there's a lot of layers to this. It isn't just one aspect.

And you have to really carefully peel through those layers, because there are a lot of interdependencies, and we don't want to negatively affect those that are doing legitimate business. We want to provide the right level of service to our customers at the same time. So, it's a fairly complex balance, and I think it will take, you know, a reasonable amount of discussion to get there, both in the industry and within the legislative community.

MR. FRANCOIS: Ms. Atkins?

MS. ATKINS: I'm not convinced Burns-Wyden -- again, the Burns-Wyden Bill goes far enough, and I don't see -- looking at the law, it's very similar to many of the state laws, and even in those states, the laws haven't had much effect. So, any law that's passed will need to be enforced, and if Burns-Wyden isn't enforced, it's no good, but I don't believe that the enforcement of the law, as it is written now, will be a trivial matter, and that in and of itself will increase expenses both for the government to prosecute, and if they do incorporate private right of action both for the ISPs and the individuals.

MR. FRANCOIS: Mr. DiGuido, economic impact of Burns-Wyden?

MR. DiGUIDO: Yeah, we think it's a good first

step. We don't believe that it is going to solve the problem. We think that the legislation is solid. We think that most of this is occurring off-shore, as my other panelists have said. We do believe there's a commercial solution to this problem. We think until there is a meeting of the minds between the ISPs, the marketers and providers, reputable providers, the problem will not go away. And it is a commercial, economic solution that will be -- that will end this problem.

MR. FRANCOIS: Lisa Pollock Mann, briefly?

MS. MANN: We believe that anything that acts as a deterrent to Spam and to help protect the online user experience is in our best interests, and we do support the Burns-Wyden Bill, because we do believe that it provides for effective deterrents, penalties and marketing rules. And really briefly, five things about it that we think does make for -- I'm losing my -- I can't speak.

MR. FRANCOIS: Now you're down to four things.

MS. MANN: Five points in it that we support. It gives users the right to say no. It gives rights to service providers to sue. It provides for criminal penalties for fraudulent e-mails, preserving service providers' anti-Spam tools and providing for a consistent national standard, because again, Spam does cross state

lines, and for all those reasons, we do believe that it is in our economic interest.

MR. FRANCOIS: Chris Lewis?

MR. LEWIS: Yeah, we see basically three issues with the bill. First of all, it's opt-out only. We believe that that might have held three or four years ago, but now, it probably would not have an appreciable effect. And any sort of opt-out legislation would have to have a global opt-out mechanism, because it is too easy to do multiple bites.

The second issue is that we would require to ban wide opt-out. One of the more interesting things is we believe that anyone that is sending porn Spam into a company is breaking the law through sexual harassment legislation, and in fact, that in many cases put the administrators and executives of the companies personally at legal risk due to the way that the legislation works in various jurisdictions. So, corporations need to be able to say, no, not only do I not want it, our whole company does not want it.

And finally, I don't think that it adequately defines providers of internet services. I've been asking around -- I didn't have access to the other legislation which actually defines what that means, but I understand that that part of the law was enacted in 1934 or

something like that, and while ISPs are obviously internet service providers, in the eyes of 877, are corporations who have their own e-mail infrastructures also ISPs? We would feel that for the purposes of an anti-Spam bill, definitely the corporations would have to have right of action against Spammers, because they're running the infrastructure. It's costing them money.

MR. FRANCOIS: Last, but not least, but with the utmost celerity, Laura Betterly.

MS. BETTERLY: I actually believe that the legislation does have to be on a Federal level as opposed to a state level. There are frivolous lawsuits, and it's very hard to ascertain when you are and aren't breaking another state law. I mean, the State of Florida, we don't have any particular laws that -- not in general, okay, just on this, okay?

(Laughter.)

MR. FRANCOIS: I am going to interrupt you there, because we need to save a little bit of time for -- and we have just that, a little bit of time for a couple of questions.

Right there. Wait for the microphone, wait for the microphone.

MR. MOORE: Charlie Moore with MailShell, and I just wanted to address a couple things. We conducted the

survey and sort of started off with Commissioner Thompson's recommendation or --

MR. FRANCOIS: Charlie, I hate to interrupt you, but I need you to get to that question, because --

MR. MOORE: Yeah, the question is really about the fear of buying online, and I think Laura brought up an excellent point, which is the 8 percent, you know, what does the 8 percent mean and that question of consumer confidence? So, really, specifically, about buying online, because our survey does say that folks are confused about what is Spam. We certainly pride ourselves on not -- on low false positives, but how do you feel about that eroding the confidence in buying online, which is such a fundamental part of the economics of the internet, and Spam is really eroding that confidence right now?

MR. DiGUIDO: You know, we work with about over a hundred reputable marketers. About half of those folks are actually doing online e-commerce. We are not hearing from them as a result of Spam thus far that there's any degradation in terms of transactions being consummated on the web. As a matter of fact, counter to that. They're seeing more and more folks spending more and more time transacting on the web. So, we haven't seen the impact. They haven't come to us and said, you know what, this

medium used to work a year ago, and today it's not working at all. They're actually saying the opposite. They're starting to spend more money and more time and more effort in terms of driving more folks online to do transactions.

MR. FRANCOIS: Laura Atkins?

MS. ATKINS: I think that there is -- there are consumers out there who are not purchasing because they do not want certain groups to have their e-mail address, and they are -- they are not making those purchases, and I can tell you, I mean, in my business, we make a lot of purchases over the internet, and there are companies that we will not purchase from. We will not purchase hardware from, we will not purchase routers from, because we cannot trust that our e-mail address will be held confidentially with that company, and that is money that those companies have lost because of that lack of consumer confidence.

MR. DiGUIDO: There are people who still don't want to give credit cards in restaurants because they're worried about someone taking their credit card number. I don't think that you can say that e-mail is any different than any other channel in terms of folks who do not want to transact with a channel because of whatever reason are not going to transact.

MS. ATKINS: No, they're specific companies. It's not the channel. We purchase -- we have made, you know, hundreds of thousands of dollars in capital investments in purchases over the internet, and the decisions of who we purchase from are based on their privacy policies and how we believe and how we perceive their consumer status. So, it's the specific companies. It is not the internet in general.

MR. FRANCOIS: We have two questions. It looks like Mona might have one from the internet, and also the gentleman in the second row after that.

MS. SPIVACK: What does the panel think about third-party programs designed to help reverse the cost model of Spam? For example, bonded sender, which requires senders to post a financial bond that gets debited if end user complaint rates exceed a certain threshold?

MR. FRANCOIS: As a caveat, we do not want to steal the thunder of the technical solutions panel, because one, that's the last panel of the forum, and they would be angry if we took away from their audience. So, who wants to address that?

MR. SMITH: I can say briefly that bonded sender, trusted sender, paying for access, all of those solutions require one thing, which is being able to

discard everybody else, and until we have infrastructure in place that allows us to recognize who's being sent in the first place, we can't do that. So, that -- the first step has got to be accountability and identifiability from senders.

MR. LEWIS: One of the other issues is that depending on who the recipient is, for example, a corporation such as ourselves, the amount of money that would be involved in borrowing an employee to market to them. I would find that most marketers would not be prepared to spend the 50 cents or a dollar each. So, you have to be -- it depends a lot on who the recipients are.

MR. FRANCOIS: The gentleman in the second row?

MR. SILVER: My name is David Silver, and I have a quick question for the FTC. I'm noticing in these panels that one constituency is missing, and that is the marketer for large corporations, and when we talk about the cost of marketing, and I think Al has done a great job in being a voice for the cost to his company in servicing marketers, but my real question is, you know, the Lands Ends of the world or the Continentals of the world or the BellSouth or let's look at Nortel, there are marketers within those companies that are using permission-based marketing techniques and sending the

very e-mail that we are having discussions about, yet they are not represented in the cost to their marketing or their ability not to market as a result of these e-mails.

I'm just curious as to when the FTC was putting this forum together, was there an effort to reach out to the key marketers, CMOs, et cetera, to hear from their point of view what their challenges are or what the cost is of not getting their marketing delivered?

MR. FRANCOIS: I will do my best to give you a governmental answer that's not an answer. We -- in terms of putting the forum together and putting panels together, we undertook the opportunity to, one, contact as many people as we could on an informational interview basis. So, to that extent, we contacted a variety of people in the Spamming community, the anti-Spamming community, the chief marketing organizations, marketers, list brokers, you name it, just to kind of cover -- get enough information for us to articulately define the issues.

And if you look at the Federal Register notice, some of the issues -- we have many more issues than we have panels, and through that process of interviewing people, we were able to whittle down what we felt were the most salient features.

To that endeavor, we did try and reach out to marketers and try and offer them a seat at the table, and I think our feeling was also that their perspective could be represented not by them necessarily specifically being here, but their sentiments could be represented best by other people.

And finally, you know, in the terms of people sending in a request for participation, we had about 225, so we were limited in who we selected to be participants and panelists, and that's kind of how we got with the composition of the panels.

In terms of what they do to market to consumers, I think that is something that can be addressed also on the best practices panel, where their perspectives will be represented there.

UNIDENTIFIED AUDIENCE MEMBER: (No microphone.) I was just questioning about -- you know, we're talking about the costs of marketing, and we aren't hearing the representation directly from that marketer, so I'm curious for the panel discussion, you talk about the problems of getting that e-mail, getting to the boss, et cetera, or opting for the information going in, but we are not hearing the other side, and I'm kind of interested in understanding from the panel's perspective, you know, from their representation, what is the cost of

not getting the messages delivered --

MR. FRANCOIS: Stan, and I hate to cut you off, but we could go on for this -- we could go on for hours, but we are out of time and currently eating into your coffee break. So, if you care to discuss it, I'm happy to.

Thank you for your time.

(Applause.)

(Whereupon, a brief recess was taken.)

MR. HUSEMAN: We are going to get started with our blacklists panel, so if everyone could please take their seats.

To begin, my name is Brian Huseman, I'm an attorney with the Division of Marketing Practices at the FTC, and this panel is going to be about blacklists. I'm going to start by reading a quote from a recent article that talks about blacklists. I'm going to ask first if you're out in the hallway if you can please shut the doors if you're not coming in. Thanks a lot.

I'm going to start by reading a quote about blacklists. It says, "Black hole lists or blacklists, databases where various organizations track IP addresses for suspected Spammers and their cohorts, there are more than 150 such lists, the most famous of which are run by SpamCop, the Mail Abuse Prevention System, MAPS, Spamhaus

and the Spam Prevention Early Warning System or SPEWS. Many top ISPs use one or more lists, blocking all mail coming from these addresses to keep Spam from reaching your inbox. The problem? Sometimes innocent bystanders or well-meaning marketers get blocked along with the bad guys, and getting unblocked can be a nightmare."

That's one person's opinion, so we are going to discuss some of these issues. Let's start off with Margie Arbon from MAPS, the Mail Abuse Prevention System. You don't like the word blacklist, do you? I think in one of our conversations, you said that that term actually almost made your skin crawl?

MS. ARBON: Yeah.

MR. HUSEMAN: Can you tell me why?

MS. ARBON: The original list was one that we had, and it was the realtime black hole list. Black hole is a router command. It was originally implemented in BGP feed, and the term came from the command black hole in a CISCO router. So, the term blacklist has kind of developed, and it's technically not what it was --

MR. HUSEMAN: Sort of a McCarthyism.

MS. ARBON: -- what it was, yes, and there's some -- it carries some emotional connotations that really it shouldn't carry.

MR. HUSEMAN: What does MAPS do?

MS. ARBON: We maintain lists of IP addresses, dynamically assigned IP addresses that are not intended to be sending mail, open relays, open proxies, IP addresses that have originated or in some way support Spamming activities.

MR. HUSEMAN: Julian Haight, you operate SpamCop. What is SpamCop?

MR. HAIGHT: It originally is a reporting service where somebody can file a complaint, and we try to identify the abuse desk responsible for the source of the e-mail they're complaining about and pass the complaint on. It has grown to include a blacklist, which is built from the data collected by that process, as well as an end-user filtering product.

MR. HUSEMAN: How does SpamCop differ from MAPS?

MR. HAIGHT: Well, the very fact that the blacklist is built dynamically in realtime from the user complaints rather than in a more judicious longer view, I think, and the realtime black hole list also has sort of a punitive motive that -- I don't know if you like that term, but you do blacklist sites that aren't actually the origination point of the e-mail but are politically connected to the origination point.

Is that correct or --

MS. ARBON: Politically connected --

MR. HAIGHT: Not politically connected but financially connected maybe.

MR. HUSEMAN: Go ahead.

MS. ARBON: We list sites that are in some way supporting the Spamming activity. Take, for example, the case that we have been talking about of open proxies. Listing the proxy is one thing, but if the same site is being advertised to the same mechanism over and over again, the site itself is a problem. The site itself is supporting the Spamming activity.

MR. HUSEMAN: Alan Murphy, you're with Spamhaus, what is your position with Spamhaus?

MR. MURPHY: I'm a volunteer. I --

MR. HUSEMAN: Speak into the microphone as well.

MR. MURPHY: I'm a volunteer. I am an editor at Spamhaus. I investigate Spam issues and make recommendations to the list.

MR. HUSEMAN: What is Spamhaus?

MR. MURPHY: Spamhaus provides two services that are widely used. One is ROKSO, the record of known Spam offenders. It's documentation really of Spammers or organizations which have been terminated for violations of acceptable use policies by at least three ISPs.

We also maintain a DNS zone, a block list, if you will, of ROKSO Spammers and other Spam sources and Spam support services.

MR. HUSEMAN: How does Spamhaus differ from SpamCop and from MAPS?

MR. MURPHY: DSBL is somewhat similar to MAPS RBL, the criteria to be entered and removed are somewhat different, but I would say substantially similar.

MR. HUSEMAN: How are they different?

MR. MURPHY: MAPS uses a various rigid, formalized nomination process. We rely more on observation of publicly available information.

MR. HUSEMAN: What type of publicly available information do you use?

MR. MURPHY: We look -- we use SpamCop statistics for one thing. We look at a number of other publicly available archives of Spam. We have our own Spam trap addresses. We know network administrators that run fairly extensive Spam traps. So, we look at a wide range of information about Spam sources and Spam support services.

And I think it's important for me to emphasize this, because this does distinguish us from SpamCop. We don't just look at the end user reports. It -- SpamCop provides a really interesting dynamic look at when Spam

hits. It requires relatively little effort to trigger a SpamCop listing, and then the SpamCop listing will deteriorate very quickly over time.

Our list is not nearly that dynamic. We need to look at a wide range of sources to determine that there really is a Spam pattern here, there really is an abuse pattern, there really is e-mail that is unsolicited and bulk, and not just identified by a single -- or a few users, a relatively small number of users, but identified across a very wide range of network sources.

MR. HUSEMAN: A question for all three of you. Who makes the decisions about what IP addresses to place on your list?

MS. ARBON: We have a nomination procedure. We also have procedures for Spam in progress or Spam that we get to our own addresses. We have an investigator that actually looks at the nomination. They require notification to the ISP. We require -- if they're in the United States, a phone call to the ISP or whoever is being listed to tell them that there is a nomination and give them an opportunity to cure. Our intent is not to list anything. We list -- we only list -- this is specifically for the RBL. We only list when there is no way to resolve the problem any other way.

After that, someone has to certify the

nomination that it does meet our criteria for listing, and then a third person has to approve it.

MR. HAIGHT: Very conservative.

MS. ARBON: Yes.

MR. HAIGHT: You try to be as conservative as possible.

On the other hand, SpamCop is at the other end of the spectrum. It's very aggressive. It's intended to actually stop as much Spam as possible, and it has the potential for problems. I recognize this.

MR. HUSEMAN: Julian, why did SpamCop choose to go the aggressive route rather than --

MR. HAIGHT: Well, because I saw other solutions that weren't effective at actually keeping Spam from my inbox. You know, if you use the realtime black hole list, you're still going to get a lot of Spam, and I was trying to find a way to stop that, and one of the things that I identified was the need to list sites within minutes of them showing up, because Spammers are morphing so fast from one IP address to another, that you really have to list the site as quickly as you possibly can in order to prevent it from getting into somebody's inbox.

MR. HUSEMAN: Alan, who makes the decisions about what IP addresses to list at Spamhaus?

MR. MURPHY: I'd like to defer on that.

MR. HUSEMAN: Is there a reason why?

MR. MURPHY: I'm currently facing litigation from my participation as a volunteer with Spamhaus.

MR. HUSEMAN: Okay. What percentage of ISPs use blacklists?

MR. HAIGHT: All of them. I mean --

MR. HUSEMAN: Every ISP uses a blacklist?

MR. HAIGHT: With very rare exceptions. We have just heard from AOL, Microsoft and Yahoo!, that they all do.

MR. HUSEMAN: What ISPs use SpamCop?

MR. HAIGHT: Ah, you know, I don't have one I can name. I don't think that most ISPs who use it want people to know that they use it.

MR. HUSEMAN: Margie, what about MAPS? What ISPs use MAPS?

MS. ARBON: We give ISPs, anybody who subscribes to our list, the opportunity to say whether or not they want to be named, and off the top of my head, I'm -- I can't think of anybody that's --

MR. HUSEMAN: Said yes to that?

MS. ARBON: -- has said yes. There are a few.

MR. HAIGHT: Nobody wants to stand up.

MS. ARBON: The smaller ones will typically say

yes.

MR. HUSEMAN: Clifton Royston (phonetic) from LavaNet (phonetic) says yes, that he uses MAPS.

MS. ARBON: Okay, thank you.

MR. HUSEMAN: Alan, what ISPs use Spamhaus?

MR. MURPHY: Again, I would probably not want to list specific names. I believe that the FTC, though, as long as we're here, I believe you use that -- Spamhaus on some of your servers at least.

MR. HUSEMAN: And I will mention that the FTC -- you are correct, the FTC has been using some blacklists recently, and we are in the process of examining blacklists and what procedures we will use for blocking and which ones to subscribe to.

MR. MURPHY: I would like to comment that it is widely used. There are probably -- by -- it's very difficult to estimate the penetration of a DNS black hole zone, because it's queried by an indeterminate number of end users and because the mirrors for the zone are not centralized. So, the estimates for Spamhaus penetration are somewhere around 100 million mailboxes protected by SBL.

MR. HUSEMAN: Why would ISPs not want to be identified as using one of your lists?

MS. ARBON: Well, one reason is it's a business

decision on the part of the ISP. I think there's probably some competitive advantage in not telling people exactly what you're doing so that you can offer a unique service to anyone else, and to be honest, with past history, I don't think they want to be targets.

MR. HAIGHT: Right, they don't want to get sued. I should also -- I just want to interject that I recommend that people use my blacklist in only an advisory mode, not to actually bounce e-mail, but in combination with other factors, to either filter it, sideline it into a junk mail folder or something like that, you know, I -- not everybody does, but that's how I recommend it's used.

MR. HUSEMAN: Let's talk now about some of the pros and cons of using blacklists. I'm going to turn now to Trevor Hughes. Trevor, you're executive director of a new association, the E-mail Service Provider Coalition.

First of all, can you tell us, what is an e-mail service provider?

MR. HUGHES: Thanks. An e-mail service provider is a company -- an e-mail service provider is a company that helps other companies send e-mail. The full breadth of the marketplace uses the power of e-mail to communicate today. It's not just marketing messages. It's transactional messages, publications, relational

messages. An e-mail service provider industry helps those companies, those organizations, those people send their volume messages.

MR. HUSEMAN: Is your coalition opposed to the use of blacklists?

MR. HUGHES: That's a really difficult question to answer in a binary form, a yes or no answer. I -- my answer is that in concept, what a blacklist is trying to do is admirable. They are trying to reduce Spam, and I think all of us recognize that that is something that we need to move towards.

In application of some of the blacklists, the related problem of false positives and some of the arbitrary and really opaque practices of blacklists cause us incredible concern.

MR. HUSEMAN: So, does your coalition encourage or discourage ISPs from using blacklists?

MR. HUGHES: I would say that currently we would discourage the use of blacklists.

MR. HUSEMAN: And, so, can you go through some of the reasons why you would do that?

MR. HUGHES: Let me give you a really -- a really clear and concise answer. Blacklists create false positives. A false positive is a legitimate message that is otherwise undelivered, and as Julian mentioned, that

he recognizes there are some problems with the blacklist -- with the use of blacklists, those problems represent what some in the community would call collateral damage. It's false positives. It's legitimate messages that otherwise aren't being delivered.

It's one thing to write off marketing messages that aren't delivered. There's a very real cost to that, and we think that's a problem, but it's not just marketing messages that we're talking about as well. It's transactional messages. It's airline ticket confirmations. It's paid newsletters that aren't being delivered. It's account transaction confirmations from your online brokerage. Those are all messages that have suffered under the blacklisting false positive problem.

MR. HUSEMAN: Okay, so talking about the reasons why you would discourage use of blacklists, you've mentioned the issue of false positives --

MR. HUGHES: Sure.

MR. HUSEMAN: -- otherwise wanted e-mail not going through and the issue of collateral damage.

Let me turn over here. Julian, are you familiar with the term collateral damage?

MR. HAIGHT: Indeed.

MR. HUSEMAN: And what would be your definition?

MR. HAIGHT: The subtle distinction between false positives and collateral damage, a false positive is something that the list maintainer somehow -- they recognize that they should not have listed something. Collateral damage is like, well, here's a site that sends a lot of legitimate e-mail and a lot of Spam, and I'm going to make a decision to block it anyway, and the messages that are legitimate from that site are now going to be blocked, but I have to because there's so much Spam also coming from the same site.

MR. HUSEMAN: Does SpamCop practice that theory?

MR. HAIGHT: Well, because it's all automated and statistical, it's not so much my decision about a site as just the volume of complaints I get about a site.

MR. HUSEMAN: Alan Murphy from Spamhaus, what would be -- are you familiar with the term collateral damage, and what would be your definition?

MR. MURPHY: Collateral damage to me is intentionally inflicting a black hole listing on IPs that are not sending Spam. The issue of mixed lists of senders that send both Spam and solicited e-mail is a gray area, and it becomes an issue of identifying which is Spam to which user, and it becomes a case-by-case evaluation in the course of the SBL.

Could I comment on the false positive issue that Trevor brought up? And that is that false positives are not simply a function of black hole lists. They're a function of any Spam filtering method. And indeed, they're even -- the SMTP system itself is not 100 percent reliable, and messages can simply get lost.

As an example of a false positive from a non-black hole list, the -- and this is somewhat humorous -- it was caught by my own Spam filters. It was a rule in my mail client that has successfully filtered out some 35,000 Spams with never a false positive before, and one of the announcements from the FTC was encoded in Base 64, and it ended up in my Spam folder.

MR. HUSEMAN: I think it was an e-mail from me to you, wasn't it?

MR. MURPHY: I believe it was.

MR. HUSEMAN: Some funny characters or something, I noticed that one, too.

MR. MURPHY: And particular to the SBL listing and false positives, I have recent figures from three large users of the SBL. One of them is NortelNetworks, you heard Chris talk earlier. In -- I believe it was in March of this year, they had an inbound on their primary mail server of about 1.9 million e-mails. Of those, the

SBL blocked 85,000. Of those -- well, it identified them. They have some processing that is beyond simply using filter. They use very elaborate, very beautifully architected mail system, but at any rate, it identified 85,000 out of 1.9 million.

Of those 85,000, 52 messages had been white listed to be desirable traffic from a particular IP address, and as a side note, I'll stress that white listing is a very important function of anybody that uses any generic black hole list. Of those 52 false positives out of 87,000, 46 were from a single IP in an escalated listing where we were inflicting collateral damage on a network in China, because that network was largely overrun by Spammers that had numerous notorious ROKSO Spammers hosted on large parts of its network, had been for months, were totally ignoring us, were not responding.

We had escalated to their corporate servers, and eventually after weeks and weeks of that, we had escalated to their entire network. That one single IP address accounted for -- which they were easily able to white list -- accounted for 46 of the 52 false positives out of 87,000 -- 85,000 total intercepted males. So, that's the sort of false positive rating that you're looking at by using what we consider to be a responsible

black list.

MR. HUSEMAN: Trevor?

MR. HUGHES: You know, the statistics, I think a lot depends on exactly what process you're looking at and when you take your picture. Some of the statistics that I have, which come from the IATFASRG, the anti-Spam research group that has been working recently, suggest that the SPEWS list, used through a Cyrosoft (phonetic), has a 53 percent rate recognizing Spam coming through in any corpora (phonetic) and an 11 percent false positive rate. So, it's a 50/50 shot as to whether it identifies Spam or not, and it's hitting one out of ten in terms of false positives.

MR. MURPHY: Yes, as I said, you need to be selective about what you use, and that's true in any market situation, and let me just finish this case by -- that rate was a 90 -- 99.7 percent correct identification, and these figures were also supported by LavaNet, who ran 163,000 realtime actual mail stream messages and also registered 99.8 percent true positives.

They also ran it on a test server that they were setting up for some other use. They ran about 10,000 messages through that. They had 100 percent true positive. And at the Spam Assassin evaluation, I believe this was also on the ASRT group, they ran 150,000

messages built from a corpus of 20 people's mail feed during the early part of this year. It contained about 45 percent Spam and 55 percent non-Spam. SBL again hit 99.7 percent true positive on the Spam -- on the mail that I identified.

MR. HUSEMAN: So, Alan, you're saying that Spamhaus, the SBL, only has a 3 percent false positive rate, is that --

MR. MURPHY: No, I am saying it has a three per thousand false positive rate according to three studies of independent Spam bodies, independent mail feeds.

MR. HUSEMAN: Three per thousand, okay.

Trevor Hughes has identified the issue of false positives as one of the problems with using blacklists. Margie, would you think that -- what is your opinion? Do you agree or disagree with that statement?

MS. ARBON: It's possible. To be honest, the most false positive complaints that we get, which I don't consider to be a false positive, it is a true positive, but, quote, "wanted mail" being blocked is, to be honest, from open proxies and open relays, not the RBL.

MR. HUSEMAN: So, you are saying that open proxies and open relays are a greater source of false positives?

MS. ARBON: But they are not false positives,

because the servers are, indeed -- have a security problem --

MR. HUSEMAN: Or collateral damage more.

MR. HAIGHT: What has been identified as false positives.

MS. ARBON: Yes, and to be honest, what the problem there is, you have a perfectly legitimate company with a mail server that either during an update or something else has managed to become open, and yes, people will complain about that mail bouncing, but we get far more on that than we do on anything on the RBL.

MR. HUSEMAN: Scott Richter from Optinrealbig, do you think that false positives are a problem with the use of blacklists?

MR. RICHTER: Yeah, and my question was actually for Alan. I was wondering what the false positive ratio is when he blocks the IP -- the host's mail servers.

MR. MURPHY: Well, the false positive rate would depend on the specific output of whatever IP address was listed.

MR. RICHTER: Well, I guess what my question is, when you block the host's corporate mail servers, what would the false positive be?

MR. MURPHY: Generally, there is very little

Spam coming out of a corporate mail server.

MR. RICHTER: So, why would it be listed?

MR. MURPHY: Because the network is pretty much overrun by Spam and not enforcing their acceptable use policy.

MR. HUSEMAN: To get the attention of the people --

MR. MURPHY: Yeah, it's to get the attention, and it's generally a very short-term thing. It generally takes a day or two.

MR. RICHTER: So, like --

MR. HUSEMAN: Scott, let me ask you a question real quick.

MR. RICHTER: Sure.

MR. HUSEMAN: Let me go back to my original question. What about the issue of false positives? In your business, have you seen that the use of blacklists is creating false positives, and is that a problem for your business?

MR. RICHTER: Yes, it's a large problem, because we believe that some of the people who do decide what should be listed and shouldn't be listed may not have the adequate skills to decipher and, you know, unfortunately some people -- you can't be a judge and a jury, unlike other organizations, where they do have a

nomination process and a little more organizational structure.

MR. HUSEMAN: Are there particular blacklists that you have greater concerns about than others?

MR. RICHTER: Well, I mean, there's obviously some lists, you know, I look at some people who run block lists and obviously aren't very proud of them, and that's probably why they wouldn't want to list and stay very secretive, and I also look at other blacklists where people do change your record and are responsible for it would not want to take credit for, you know, being responsible.

MR. HUSEMAN: Okay. So, we've identified the issue of false positives as an issue in the use of blacklists. Someone has also identified the issue of collateral damage as being another issue.

Cindy Cohn with the Electronic Frontier Foundation, if I'm correct, your organization believes in the privacy of the First Amendment. How does that --

MS. COHN: That's why it's the first one.

MR. HUSEMAN: How does that view affect your view of blacklists?

MS. COHN: Well, I'm -- I think I'm a rarity here, because I'm not actually here representing a company or a business. I'm here because EFF has received

complaints from non-commercial list serve owners that they have an ongoing continual problem getting their solicited messages through because of various Spam mechanisms. Blacklists are not the only problem.

And looking closely at the mechanisms and the ways that all of these things are being blocked, as a First Amendment lawyer, I see a lot of things that frankly are traditional First Amendment problems in the way that the anti-Spam mechanisms work. Lack of transparency in the system, overbreadth, failure of due process, so that if you get listed, you can't even know in some situations who it is you go to to try to get off the list, and then misuse of the list for improper purposes.

Now, these are the sorts of things that would be really an easy case for me to win should a government entity do that in terms of trying to decide what speech is allowed and what speech is not allowed, and while there are significant differences between governmental entities and non-governmental entities, both legally and I think as a practical matter, I think it's reasonable to question whether there's some basic fairness and real problems here when these clear problems exist even in a non-governmental context.

MR. HUSEMAN: Cindy, I think you made a couple

of really big points, so let's add to our list of cons against using blacklists lack of transparency, overbreadth, lack of due process and misuse of the list for improper purposes.

Margie, what is your response to those four new issues that Cindy raised? And let's start with the lack of transparency in some blacklists.

MS. ARBON: The bottom line is blacklists are a decision by the owner of the equipment that the mail is going to. We are running a balancing act between property rights and First Amendment rights. You have people that are trying to maintain service, they are trying to maintain a business. I've seen cases where servers have been cascaded by the volume of mail coming through them that may or may not have been solicited but was definitely bulk, cases of a small ISP that was almost completely put in bankruptcy because they had an unfortunate name. They are defending their property. They are trying to be able to maintain a business model, maintain a correct, proper service, and they're being inundated by that mail.

The advantage of a black hole type list or DNS-based list over a lot of the other filtering mechanisms is the content of the mail never actually hits the server. In most cases, it's -- we had the

demonstration on e-mail yesterday. It's rejected after the recipient, too. So, if you have a -- and I've seen them -- 900-megabyte or 900-kilobyte Spam coming through, the receiving server doesn't actually have to accept that mail. It can bounce it back and say no, this is coming from an IP that I'm not willing to receive mail from.

MR. HUSEMAN: It saves bandwidth.

MS. ARBON: What's that?

MR. HUSEMAN: It saves bandwidth.

MS. ARBON: Who were her other --

MR. HUSEMAN: Well, let's go to Scott Richter. What about the lack of transparency in blacklists? Let me ask you a question. Are some of your IP addresses listed on various blacklists?

MR. RICHTER: Yes.

MR. HUSEMAN: What is -- do you see that the -- do you see a problem with lack of transparency as far as standards and having your IP addresses listed?

MR. RICHTER: I believe that in any ISP, if they want to block us, that's their decision, but when we have relationships and we work with ISPs, we can also, you know, come to an agreement or we can work to solve the problem.

The problem, when you're dealing with a new --

a wide range of blacklisting products is they're all so random. You have one person who hides and throws eggs. You have one person who has volunteers who have no guidelines and will basically list whatever information they feel like listing on you, personal, private, you know, doesn't -- doesn't phase them. And then you have another blacklist where they don't -- you know, divulge that anyone can send complaints, you know, they can -- anyone can join and sign up.

There is no proof whether these people who are submitting the complaints really are getting Spam. I mean, nobody really knows. With a lot of programs now, it's all automated, where they just forward their entire inbox to the program. You know, and then we think we have one true blacklist where at least they take accountability for it and, you know, have a nomination process and, you know, call you up in advance and, you know, tell you what you've done or, you know, how to solve it or, you know, and are willing to work with you, and I think that, you know, there's a big difference. You have, you know, four different, you know, major blacklisting groups that have such a wide range of diversity.

MR. HUSEMAN: Julian Haight, your opinion on the transparency and standards? As Scott Richter

mentioned, many systems or several blacklists I guess, probably yours principally, uses an automated-based system.

MR. HAIGHT: Right.

MR. HUSEMAN: How can -- if it's automated and complaint-driven, how can a business or marketer know what conduct they are doing will have them end up on your list?

MR. HAIGHT: Okay, two different questions.

The -- as far as the transparency goes, I do try to be accountable and transparent in my listing criteria. The listing criteria is based on these user complaints, so it may still be unpredictable. So, you know, I don't know -- I guess what I would say to Scott is that we know at least when someone files a complaint about you that they did receive an e-mail from you if they perceive it as Spam. I guess, you know, I --

MR. RICHTER: I think with some products now, you know, for instance, Spam --

MR. HAIGHT: Just speaking for my own products.

MR. RICHTER: Yeah. I mean, on some of your products, it's automated now?

MR. HAIGHT: Well, the whole -- I mean, it is fully automated.

MR. RICHTER: And you're tied in with McCaffrey

(phonetic) now, right?

MR. HAIGHT: No, I --

MR. RICHTER: Or I know some users forward like their entire inbox and --

MS. ARBON: That's Spamkiller.

MR. RICHTER: Okay, Spamkiller.

MS. COHN: I have one thing I'd just like to toss into the mix about accountability and basing it on user complaints. One of the things that is of concern to us, I work with, again, some of the really large list serves that do political activism online, which I view as one of the tremendous benefits of the internet, is its ability to allow people to do political organizing online, much cheaper, more efficiently. One of the ones I work with is Moveon.org.

They are quite concerned that the complaint-driven Spam lists are actually being gamed by people who have a political problem with the content of their messages, and I -- you know, while I in general like to empower the recipient to do things, I am quite concerned about the misuse of some of these complaint-driven mechanisms for really what is censorship and content-based discrimination.

MR. HAIGHT: In cases like that, I am available and willing to make an exception, if necessary, or to

take action to stop that use of my system. I wouldn't support that.

MR. HUSEMAN: Alan Murphy, what is your --

MS. COHN: Can I just add one last thing? Because the other piece of all of this is, of course, it's very difficult to know why the list serve owners why they are being blocked if the ISPs aren't being honest about who's doing the blocking. So, how is my, you know, little guy who's running a list serve, the Berkeley High School list serve is getting blocked, how do they know that they need to contact you?

MR. HAIGHT: Because every time their mail is rejected, a bounce is sent back to them with a URL going to my site where they can get more information, and if somebody is not providing that bounce back -- well, if they're sending to a large list, at least some percentage of the recipient servers are going to provide that. If they run into a situation where that's not happening, well, it's out of my hands. That's the receiving server's problem.

MR. HUSEMAN: Alan Murphy, what is your response to Cindy Cohn's point that some lists are misused for improper purposes?

MR. MURPHY: I think the way to address that is looking at a definition of Spam, and I'm on a number of

Spam -- anti-Spam mailing lists by my own opt-in choice, I'm on these lists, and sometimes I wonder about the volume of mail that I receive due to these discussions and how worthwhile it is to read for about the 5000th time that -- what is Spam?

And Spam comes down to essentially unsolicited bulk e-mail, and just briefly commenting on a lot of the legislation that's been proposed, it looks at content, it looks at fraud, and I understand some of the reasons for looking at that, and it actually touches on Cindy's point, because the Government does not want to interfere with free speech, and I'm an adamant proponent of free speech. So, I understand why the Government wants to regulate that way.

But unfortunately, it doesn't address the basic issue of unsolicited bulk e-mail, and one of the things about a black hole list is it is very content-neutral. The only way it touches on content is if the publisher of the content uses a particular IP. All the list cares about is that the IP, in Spamhaus' case, that the IP either sends or supports unsolicited bulk e-mail. That's our basic criteria.

MR. HUSEMAN: Scott Richter?

MR. RICHTER: Yes, my question was about something that I had noticed on the person that posted

-- who I know that even I think SpamCop at one point was using their records, their blacklist to query, about working to get off these blacklists, and the person's comment was when I pressed Julian to do the decent thing to clear my name and to set the public record straight, Julian flatly refused, providing me only with the excuse that he felt that he had to fully maintain at all times on the SpamCop website even evidence of SpamCop's own clear mistakes for the sake of having a complete historical record of these mistakes.

MR. HAIGHT: This was -- if I recall, this was a situation where somebody had been blocked wrongly, we reversed it or somehow corrected it, and I suppose to this day that IP address shows a listing history which says when the IP address had been blacklisted previously, right, and I don't see a reason to erase that record.

MR. HUSEMAN: Let me move on to a different topic real quick.

Trevor Hughes, the lack of due process in being removed from some of the lists has been an issue that was raised. What experience have e-mail service providers had on this issue?

MR. HUGHES: They have had a terrible experience. I -- it's related to the transparency or, rather, the opacity issue that we're talking about here,

and I actually do have to commend Alan, Julian and Margie for being here, because that is a big indication that they want to be held accountable for what they're doing.

We do have blacklists out there where people don't want to be held accountable for what they're doing, where they have no identity, where the standards are arbitrary and, in fact, they shift, and if you are listed on the blacklist, the due process associated with being removed from that blacklist is unknowable. In fact, in some situations, you have to post on a public news group in order to raise your concern and essentially expose your problem for the entire world, whether or not it's a real problem.

So, the due process issue is very real. The experience of e-mail service providers with the due process issue with blacklists is an incredible concern, and I think it's very related to the accountability and transparency issue that we've just been discussing.

MR. HUSEMAN: Margie, what is your view about any due process concerns?

MS. ARBON: There's always another alternate route. All of these lists are DNS-based. The DNS configuration, the mail server configuration, is done by the ISP. You know who's blocking the mail. You know where you can go. If X domain is rejecting your mail

based on a list that you can't contact the operator, you can always contact the ISP or corporation or whoever is using the list and ask them to white list you.

MR. HUSEMAN: Or discontinue the use of that list.

MR. HUGHES: Right, you know, if I could, my members -- some of them had no one working on ISP relationships 18 months ago. Many of them now have a number of people working on ISP relationships today, and it is for exactly that reason that many of the blacklisting issues that they face, their only recourse is to work with the ISPs. But in that situation, the question is is that the right place to resolve the issue?

It is spreading the problem across literally thousands of ISPs, thousands of corporate mail gateways or mail gateways period as opposed to resolving it at the source of the problem, where the listing occurs, and that's at the blacklist.

MR. HUSEMAN: Margie?

MR. HAIGHT: Well, the alternate side of that, if I may -- go ahead, Margie, if you like.

MS. ARBON: You do have a point. It is much, much easier to deal with the list operator. On the other hand, the fact that people that are sending large quantities of bulk e-mail to ISPs, whether it be

solicited, unsolicited or anything else, that have no relationship with the ISPs that they are sending large quantities of mail into is disturbing.

MR. HAIGHT: Right. I mean, all of these people or all of these thousands of sites are likemind, I understand their desire to not receive the Spam. So, if you want to send them the -- well, the supposed Spam or the alleged Spam, then you should have to contact them and say, hey, white list me. I mean, if -- well, I'll leave it at that.

MR. HUGHES: We heard on the previous panel, though, that there are many ISPs that have no resources for those type of connections, that once you get past the -- say the top ten ISPs, that those types of interfaces do not exist. They need to buy something off the shelf that is easy for them to resolve, and over and above that, we see corporate mail gateways, we see educational mail gateways, where there are no resources for dealing with those types of interactions.

MS. ARBON: There has to be a postmaster.

MR. HUSEMAN: Scott Richter, what has been your experience in dealing with ISPs for IP -- your IP addresses that have been listed?

MR. RICHTER: We have had actually a very high success rate in being white listed at the ISPs. The --

you know, the biggest thing is is it's -- you know, it's just an extra hassle and an extra step for us to have to undertake. It's not that it's -- you know, like I said, it's just adding an extra, you know, process.

MR. HUSEMAN: Your comment was ominous, it made the lights go down.

MR. HAIGHT: I would say that's a cost of doing that type of business.

MS. COHN: Yeah, but the people that I'm working with aren't about cost, right? I mean, the problem is that if you build a system that you assume that all the people who are participating in are commercial entities with commercial business links, that's fine, but, you know, the thing again about the internet was that it was a -- you know, it started out as the great democratizer so that you could be three people in a garage who all had day jobs and still run a very large list serve.

David Farber (phonetic), who's on our board, created the very first list serve on the internet. It's amazing, every time I talk to Dave Farber about something, he always did it first, but, you know, he's got a job and a life, and he spends an inordinate amount of time trying to make sure that his messages get through to his list, and it's a noncommercial, completely opt-in,

private list. So, I think you need to think about solutions that work for people who don't have resources as well or else we will have lost one of the more amazing and important pieces of the internet.

MR. HUSEMAN: Trevor?

MR. MURPHY: Absolutely, but why would people be using those lists in the first place if it -- that caused that damage if there wasn't a huge problem to begin with?

MR. HUSEMAN: Trevor Hughes?

MR. HUGHES: First, to Alan's point, I think we're all here because we recognize the damage that Spam is causing, and if we don't resolve the Spam problem, that, you know, we will not be enjoying e-mail the way we are today two years from now.

But I do want to respond to Julian's point about purported Spam or --

MR. HAIGHT: Alleged Spam.

MR. HUGHES: -- unsolicited commercial e-mail or marketing messages. We're not just talking about marketing messages. We're talking about the full breadth of communication in society today. We're talking about transactional messages. We're talking about relational messages. These are much higher-value messages, and blacklists do not discriminate on a content basis. They

are wiping them clean across the board.

MR. HUSEMAN: I'm now going to go to one specific list that has been alluded to now, that's the SPEWS list, the Spam Prevention Early Warning System. Julian, what is SPEWS and what do they do?

MR. HAIGHT: Okay, I just quickly want to respond to that and say that these messages will only get mixed, assuming that the same sender is sending their transactional mail and their unsolicited bulk e-mail from the same exact IP address or -- I don't know, I guess depending on the blacklist, but that if you mix your messages, then you're going to lose -- you're putting all your eggs in one basket basically.

Okay, I'm sorry, could you repeat your question?

MR. HUSEMAN: Now getting to the topic of the SPEWS list in particular, what is SPEWS and what do they do?

MR. HAIGHT: Okay, well, I'm not with them, but I will try to put forward their argument. I'm not sure I support it myself, but I think the argument is sort of going back to what Margie was saying about the recipient mail administrator -- that mail server being their property and that if they want to use a list that has those policies that is not accountable, is not available

for discussion like this, that that's their right and that the publishers of the list are --

MR. HUSEMAN: Can you describe a little background, please, what SPEWS is?

MR. HAIGHT: All right, it's a blacklist -- well, nobody really knows who's running it. We knew the domain is SPEWS.org, I think that's it, but above that, there's really not a whole lot of information. If you have a problem with being on the list, you're instructed to post to the Spam news group, basically outlining the problem and making a case for why you shouldn't be on the list, and presumably the people who are on the list monitor that news group to see these types of things, but who knows? And nobody knows, at least nobody I know knows, who's behind it.

MR. HUSEMAN: Scott Richter, you don't like SPEWS, do you?

(Laughter.)

MR. HAIGHT: But that speaks very well of it that Scott does not like it.

MR. HUSEMAN: Scott, what is your view of SPEWS?

MR. RICHTER: You know, I probably should let that one go by for now.

MR. HUSEMAN: Okay, Cindy Cohn, do you have a

-- does EFF have a position on SPEWS?

MS. COHN: Not really. We don't generally take positions on particular products and services. We try and -- try not it. What we're trying to do is focus on the principles. I think that, you know, my concerns about the SPEWS list really fit very well in the general concerns I have here, the transparency --

MR. HAIGHT: Well, let me outline their position in terms of the First Amendment, that they have the right to publish this list, you know, and people have the right to use it for whatever they want.

MS. COHN: Yeah, I think that, you know, there's an argument there, but I think that you can't ignore the effect of what you're doing. You can't just, you know, well, I have the right to say this, and the fact that, you know, we had to kill the internet in order to save it is just a side effect of me exercising my First Amendment rights. I'm a big fan of First Amendment rights, and I recognize the difference between a governmental censorship scheme and a private censorship scheme, but I'm quite concerned about the effect on the end-to-end nature and the open architecture of the internet with, you know, private entities and anonymous entities deciding which of your mail gets through and which of your mail doesn't get through.

I think one of the things that concerns me a bit about some of the Spam debates is that it appears to assume a world in which the only people who matter are sys admins and ISPs and that end users are not, you know, important, and so it's okay to blacklist an entire domain, despite the fact that lots of people who are sending mail through that domain and use that service are not actually engaging in illegal behavior, but simply just aren't getting their mail delivered or their mail received.

MR. HAIGHT: What about the argument that this is similar to a restaurant reviewer, say anonymously saying, don't eat at Joe's, I got sick? How is this different?

MR. RICHTER: The restaurant reviewer doesn't block the entire street.

(Laughter.)

MS. COHN: Yeah, I think that's one argument.

MR. HAIGHT: But we're not blocking the intermediate area routers between the sender and the recipient. The recipient is making the decision or the recipient's sys admin is making the decision.

MS. COHN: Yeah, I think that's an important distinction, and it's one that we need to pay a little more attention to than I hear sometimes. You know, I

love sys admins, I'm with the Electronic Frontier Foundation, for God's sake, but this kind of -- I hate to do this, but, you know, this kind of morlock (phonetic) view of the world, right, that we only talk to other people who are like us, and so we'll all decide, I think is having some major collateral damage for end users, you know, and I think that if you're responsible and you're moral and you recognize that what you're doing is processing speech, you'll think a little harder about trying to make sure that you are careful in making sure that you don't prevent the speech of, you know, people who aren't violating your rules as a side effect of trying to get at the people who are trying to violate your rules.

Again, if the Government tried to do this in a censorship scheme, it would be a slam-dunk easy case for me, and if the harms are the same, then maybe you have a moral obligation to think a little more carefully about your techniques.

MR. HUSEMAN: I do have one announcement. Security has informed me that we cannot block the doorway entrances, so if those of you standing could just please move away from the doorways themselves. Thank you very much.

Okay, getting back to our discussion, let's

talk about the issue of best practices for blacklists. I'm going to go back to Cindy really quickly. EFF has been working or has developed a list of best practices for blacklists. Is that correct?

MS. COHN: Well, we're starting a list of principles and best practices that actually is trying to encompass the problems of noncommercial list serve owners and their best practices as well as those of ISPs and people who are taking it upon their selves to try to do anti-Spam things, and it's a work in progress.

We're just starting, actually, because the -- some of the problems that we're -- you know, what happened was I got a call from Moveon, they said they were having trouble getting their servers, you know, their messages through, and I sent a little note out in EFF's newsletter, which, by the way, has a continual problem with Spam filters, because we cover Spam issue and we talk about porn, because we cover those issues, and I don't think we're a legitimate target of any of the filters, but we have a continual problem trying to get through.

But asking for noncommercial list serve owners to tell me if they were having trouble with Spam filters, and the reason I'm here today was because I got an overwhelming response. I got high school newsletters. I

got, you know, Dave Farber, the first list serve ever on the list. I got people from all sides and scopes of noncommercial, you know, completely opt-in sorts of list serves who were having trouble with Spam filters, and that's when I decided that perhaps we were fundamentally starting to break the internet and that it was time for the EFF to actually participate.

So, we're starting a list of how to work through the best practices. It's not easy and it's a work in progress. So, if folks are interested in assisting -- and again, I'm focusing on noncommercial list serves now, because I can't take on the whole thing, but I would be willing to talk with folks.

MR. HAIGHT: I certainly agree with what you're saying, and my concern is just that the -- that organizations like ours are legislated out of business or out of existence even if it's not a business.

NEW SPEAKER: Or litigated.

MR. HAIGHT: You know, I agree with all the concerns you're raising. It's just that these filtering technologies are our last resort to save this medium.

MR. HUSEMAN: Let's move on to -- speaking of some of these issues, moving on to another topic. Let's talk about some of the legal issues involved with blacklists. Let me turn to Stuart Ingis with Piper

Rudnick, an outside counsel to the DMA. There have been several lawsuits involving blacklists. As Alan Murphy, one of our panelists said, he is an individual defendant in one of the lawsuits that has recently been filed. MAPS has been the subject of previous lawsuits.

What is your view -- and there have been several causes of action as the basis of these suits. One has been defamation and another has been tortuous interference with contract. Does the use of blacklists by blacklist operators amount to a tortuous interference with contract?

MR. INGIS: Well, let me step back a second before answering that, and I think that it's important when you look at the litigations that have gone on to see what steps it is before you get to the litigation, why it is that you're at the litigation. I think we've kind of covered some of that here, which is in the cases of all of the lawsuits that have happened, where there are legitimate communications where the consumer wants to receive it and the sender wants it to get to the sender that have been blocked by blacklists, in full recognition that there are, you know, good values to a lot of blacklists, and then they try and resolve their complaints, and in many instances, I think a lot of the varying blacklists, if you can find them, do resolve the

complaints.

But then there are the instances where you can't resolve the complaints, and so in that instance, you use your last resort, which is litigation, and to answer the question, there are really -- there have been three areas in litigation that have been used. One is tortuous interference with contractual relations. Another is defamation and another is more of an antitrust concept. I think on all three of those areas, and we can get into, if you want, into the specific criteria to establish the violations, but I think that they're all fact-sensitive, and they're really determinant based on what types of communications are actually being blocked, where the different contracts are.

In the case of contractual -- tortuous interference with contractual relations, there are really three different types of contracts that I think have come up in these cases that the argument is that MAPS and its -- and some of the other blacklists, MAPS really has been the subject of most of the litigation, although a lot of that is a couple of years old now, but there are several different types of contracts that are blocked.

One is among the ISP that's providing service for a sender of the message and that sender, because no longer are the messages being sent, and somebody has paid

a significant amount of money to be able to send those messages. Another is between the sender of the message and the consumer, the customer, and, you know, as Trevor has stated very well, it's not just solicitations we're talking about here. It's bank statements, it's, you know, I want the New York Times delivered via e-mail to me every day, and so it's those types of communications, and so those contracts, there's an interference with that relationship.

And then there's a relationship in some cases between the sender and the e-mail service provider, so that the person who wants the communication to go out in an instance where they contract with the service provider, they've contracted, you know, for the service provider to -- for a significant amount of money to deliver these messages, which are no longer being delivered. And so, those are the types of contracts we're talking about.

MR. HUSEMAN: Would the cause of action be against -- tortuous interference with the contract be against the blacklist operator or against the internet service provider that is using the blacklist?

MR. INGIS: I think both is the answer. It can go both ways. In the instance of the blacklists, one particular scenario which I think really is the most

egregious when you're looking at the contractual relation is when there are IP -- there are senders that use the same IP address but are totally unrelated to the sender of the message that ultimately has caused the IP address to be put on a list, and that particular sender has a relationship with an ISP, and all of a sudden, their messages aren't getting delivered, and they had -- they weren't even the accused message.

MR. HUSEMAN: Have there been actions so far against ISPs that have used a list to date?

MR. INGIS: A lot of the actions have named multiple parties, the blacklists and the ISPs, and interestingly, a lot of them settled fairly quickly with some of the ISPs and almost in a white list type of concept, which may be, you know, as we start talking about solutions later in the other panels, you know, it may be part of a solution to some of the excesses that you see in blacklists.

MR. HUSEMAN: Michael Grow, you are an attorney and have been involved in the anti-Spam field for quite some time. What is your view about the legal theory that either operating the blacklist or an ISP that uses a blacklist is involved with a tortuous interference with contract?

MR. GROW: Well, I have a different view. I

think it's like saying to those restaurants which require you to wear a coat and tie that you're interfering with business relationships among people who want to go there and talk to each other. I think you have to step back and understand that blacklisting exists only because ISPs are trying to protect their own business interests. If the ISPs didn't use a blacklist, you know, nobody would be here today, and the ISPs, because they've made an investment in this equipment and because they've got customers who object to unsolicited bulk e-mail choose to use blacklists as one means of protecting their customers against this sort of thing, and they have a perfect right to set whatever standards they want with respect to the type of use that their equipment will be put to.

So, I don't think there's liability on the part of either the blacklist or the ISP who chooses to use this under a tortuous interference theory.

MR. HUSEMAN: Is publishing a list of IP addresses of known or suspected Spammers, would that be defamation?

MR. GROW: Well, I don't think so. I mean, it depends, first of all, on what standards you use to publish the list. I think if you knowingly put someone on a list, knowing that they're not a source of Spam, and you've made a false statement and that causes damage to

someone, that may be actionable, but if you conduct --

MR. HUSEMAN: Can you speak into the microphone?

MR. GROW: Oh, I'm sorry, I'm sorry.

I think if you conduct a reasonable investigation and you determine or you form an opinion that someone is a source of Spam or that a particular internet protocol address is being used to send or relay Spam, there's a First Amendment right that attaches to that as well, and if you have a right to express your opinion in an e-mail, you've also got a right to express an opinion about those who send that e-mail and as to whether or not it constitutes Spam.

MR. HUSEMAN: Scott Richter?

MR. RICHTER: My question for Michael, what -- when a blacklist provider let's say lists the corporate mail servers and ISP, would that -- and let's say the ISP, let's say they're very large and they have, you know, many customers, and they're listing them for the sole purpose of, you know, because they want somebody to be terminated, would that be damageable to the blacklist then?

MR. GROW: Well, yeah, I'm sure from that person's perspective, there's damage any time somebody's listed on a blacklist, but I think this is really more of

a marketplace issue than a legal question. People who go to a particular ISP do so for a number of reasons, but one primary reason today is that that ISP is providing some kind of Spam filter protection. If they don't get that kind of protection, they're likely to leave that ISP and go somewhere else.

On the other hand, if somebody is not getting e-mail that they want, they may leave the ISP for that reason. So, the ISP's got to make a business decision as to how it crafts itself.

People who send e-mail have the same business decision to make. If they want to ensure their mail goes through, they won't use their corporate e-mail account to send unsolicited bulk e-mail. They'll use some separate IP address.

MR. HUSEMAN: Trevor Hughes, can you respond to that question? If a customer has an issue with false positives or does not like their mail being blocked by their ISP, why can't they simply switch ISPs in the marketplace?

MR. HUGHES: They can. They can. We all know that there's a cost to that churn, though, both for the recipient of the e-mails and for the ISPs.

You know, I -- one of the concerns that I continue to have, and I'm not hearing a satisfactory

resolution to today, is that we're not hearing about accountability from the blacklists. A blacklist demands accountability from the sender community, but the inverse is that -- or the flip side is that there's not a recognition or a willingness to accept accountability for the practices of the blacklist.

Now, SPEWS obviously is the most egregious example of that, but if blacklists are to demand accountability, I think they should be held to that same standard.

MR. HUSEMAN: Alan Murphy, what's your response to that?

MR. MURPHY: I'm not particularly clear on what it is that Trevor says we're not responsible for or not transparent about.

MR. HUSEMAN: We are here trying to take responsibility and be accountable --

MR. MURPHY: Actually, I have a comment relating to that that goes back to Cindy's talking about a best practices document, and I think that's a wonderful thing. I don't think it should be a -- well, let me -- on the internet, the internet is specified in a series of documents called RFCs, and you don't have -- no one has to follow an RFC. They're suggested best practice. And one of the RFCs goes as far as to define the words

"should" and "must." I think we can all use them in common context here.

I think a best practices document should be a part of block hole lists. I think that if a block hole -- if a person wants to run a DNS zone that is designed to block e-mail and they don't want to follow current best practices, it should be like the RFCs, they don't have to do it.

Now, whether or not anybody wishes to exchange traffic with that particular black hole list becomes a market decision, and my personal recommendation to an ISP or a business would be to not use a black hole zone that does not follow good practices, and if there were a document of current best practices with which I agreed, I would recommend they follow that document.

MR. HUSEMAN: I want to get back to the legal issue briefly about defamation. Stuart Ingis, what is your response or what is your view about the defamation theory?

MR. INGIS: Well, I think the defamation theory actually kind of comes down to the type of message. I think there is message under, you know, any -- or numerous definitions that is Spam, and if that is blocked and you're called a Spammer, then there's really nothing defamatory about that.

However, the perception, when a lot of messages -- legitimate messages are blocked, bank statements, you know, your New York Times, you know, daily e-mail and even solicitations that have been asked for by consumers, if those are blocked and the theory by which they're blocked that all of the lists are providing is that they're Spammers, and in fact, they're not, these are legitimate communications that are wanted and they don't have the derogatory meaning, then I think that there is some defamation and defamatory result.

MR. HUSEMAN: Cindy Cohn?

MS. COHN: I just wanted to jump back a second to the idea that customers can switch ISPs if they don't like how the Spam blocking is working and just highlight a problem that came up in my investigation of this, which was that there's an interesting problem with some of the feedback loops for ISPs, which is that they don't actually -- recipients don't often know when they're not getting their mail. In fact, the whole moveon.org incident arose because someone who is a large fan of the organization wrote an extremely nasty e-mail to them saying, you guys dropped me, you know, I love you guys and you dropped me, I can't believe it, and, you know, sure enough, it turned out that the ISP, in that case AOL, had just not -- you know, had decided that this

was -- that it was a Spam and had not delivered the mail.

So, there was an interesting feedback loop issue, because I think recipients often know -- you know, always know pretty much when they get something that they don't want, and I think there's less -- there's less ability for a recipient to learn what it is they're not receiving, and so the ISP ends up hearing all about the Spam and very seldom hearing about the legitimate e-mails that get thrown away.

MR. HUSEMAN: Julian Haight, is that an issue about senders of e-mail not knowing if their e-mail got through or recipients not knowing if they did not receive an e-mail?

MR. HAIGHT: Yeah, it certainly is, but sort of the bigger issue here is that e-mail has for a long time seemed free, but it really isn't, and that the senders of e-mail, like you're talking about, who have real jobs and don't have a lot of money to spend on this are sort of freeloading and that at some point those costs have to be paid.

If the recipient wants, they can pay to get an unfiltered e-mail account, and then they can get all their Spam, everything, or design the filters as they choose, but with a situation where you have free Yahoo!

accounts and people who are sending using a small account at an ISP, the cost is sort of built into the recipient's e-mail, but it's also saying, but we're going to filter out some of the e-mail because -- you know, and this is sort of built into the user's agreement with their ISP, that the ISP is going to do this filtering or at least it should be built into the agreement with the ISP, that the ISP says, well, we're going to do this filtering, it's on a best effort basis, and if you don't want that, you're going to have to pay more, because it's going to cost more.

MR. HUSEMAN: Scott Richter, what's your response?

MR. RICHTER: Well, as far as the costs and I think also with the first question, I was just wondering -- I was noticing that on your people who use SpamCop to block and with the recipient, I think a lot of times the recipient -- obviously a mail sender is sending the mail, they always should know if their mail doesn't get delivered for the most part, they should receive a message back, but a lot of these recipients -- and you brought up the fact of if you want all your mail, go to a paid service, but a lot of the paid services still use filtering, Hotmail, MSN, Yahoo!, AOL, I mean, they're all paid services, and they have filtering that the end

recipient may not know that he is receiving, but I guess my biggest question is, I notice on your site it says, you know, do not use this, just in beta testing. I mean, do you think that there's some risk in that, having a product out that shouldn't -- you know, that you're kind of saying not to use that people are?

MR. HAIGHT: What's the question?

MR. RICHTER: I was wondering if the -- on the website it says to -- I think the product is in beta testing, you know, not to use, you know, because it could affect e-mail delivery. Do you think there's a danger knowing that some medium-sized ISPs are using the product knowing that there's some issues with it?

MR. HAIGHT: Well, I think the users expect their mail to be filtered by their ISP and that if it weren't, they would be more upset than they are at losing some e-mail that they do want, at least in the proportions that they are. Yeah, I agree that if somebody absolutely must receive e-mail, then they shouldn't be using any sort of filter and that users should be aware that ISPs are doing that filtering, and I think by and large they are, and they like it.

MR. HUSEMAN: Alan, your response on this issue, and then we'll move on to another topic, about not knowing whether you did not receive e-mail or not knowing

whether your e-mail was actually sent?

MR. MURPHY: Yes, exactly. As Cindy pointed out and also as Scott touched on, while a lot of the blocking can go on from any sort of filtering list, not just a DNS blocking list, it could be content filters or a variety of other filters, any of those methods can be used to bounce e-mail, but by default configuration, black hole lists are at the server level, automatically return an error message that can be read by the sender, and that is not true for many content filters. While they can be configured into a mail server that way, the default configuration is often not done that way, and other method -- other filtering methodologies do not have that feedback loop built into them.

MR. HAIGHT: That's as far as the sender goes.

MR. HUSEMAN: As far as the sender goes was your point, Julian.

I want to touch on the last legal issue, and that is about the antitrust and illegal restraint of trade issue. Stuart, what is your viewpoint on that?

MR. INGIS: Well, it's a very complicated issue, so just briefly, there's -- there are a couple of concepts that would need to be shown. One is that there's an agreement among internet service providers, and to show that, you can show a contract between all the

ISPs and a black list, which probably doesn't exist here, or there are other indications that you can show that there are a series of agreements, and everyone kind of knows that the others are acting this way and put people on the list with that knowledge, and I think that that probably could be shown.

Then you need to get into the second, broader element, which is whether there's a what's called per se violation or rule of reason, and the interesting question really on the per se analysis, and then I'll stop boring people with the legal terminology, but is really whether there's market power among the ISPs, and I think that the antitrust lawyers in our firm that I've spoken with about this say that, you know, the internet raises particularly interesting questions as to what is market power, because you only really need to have one entity kind of on the whole broader internet or one piece of the backbone -- in some instances, not all instances -- routing messages off into the black hole or off into, you know, nondelivery land, and so the result of that is it doesn't take, you know, but one individual theoretically, you know, as you heard, well, you know, if there's a problem, you can contact me, you know, and I'll address that, to exercise significant market power.

So, I think that, you know, the issue hasn't

been resolved by the courts, but I think that that really is what it would hinge on in that type of analysis.

MR. HUSEMAN: Michael Grow, your response briefly before we break for questions?

MR. GROW: I don't think the antitrust laws apply to this at all. I think they're set up initially or in corpus to prevent unlawful conspiracies that restrain trade, and there is an exemption for joint activity where it's noncommercially motivated and it's aimed at achieving some social or political goal. Most of the blacklists and other anti-Spam organizations are actively involved in trying to promote legislation that will prevent this type of activity. So, the fact that there may be multiple blacklists or ISPs that use them I don't think gives rise to anything.

The antitrust laws have also long recognized that businesses are free to act independently and to choose who they will deal with, and that's exactly what ISPs do when they choose to use a Spam filtering device or a blacklist. And a group boycott can only be per se unlawful if it applies to horizontal agreements among direct competitors. Generally, these agreements are not among competitors. The ISPs may be trying to protect themselves, but they're not aimed -- their agreements or whatever they may be are not aimed at other ISPs.

They're aimed at people who send Spam. So, it doesn't apply in that regard.

So, the rule of reason analysis is what would be applied if there were an antitrust argument, and in that case, the person bringing the claim would have to show that there's an adverse effect, a significant adverse effect, on competition in a particular market, and even if there is, then they have to show that the pro-competitive -- whether or not the pro-competitive benefits outweigh the anti-competitive benefits. There's significant pro-competitive benefits in blocking Spam or using a blacklist. In fact, without some kind of blocking or filtering, ISPs wouldn't be able to compete. They'd all be out of business.

MR. HUSEMAN: We are now going to take questions for our last 15 minutes from the audience. Yeah, great.

Sir, standing up right there?

MR. FELSTEIN: My name is Mark Felstein. I represent emarketersamerica -- my name is Mark Felstein. I represent emarketersamerica.org, and I represent, and I am the gentleman that just filed the lawsuit against Spamhaus and SPEWS and several other individuals, and my question, which I hope that Mr. Murphy will answer, is that in his definition of collateral damage, he defined

it as intentionally inflicting a blacklisting upon an innocent, and then he went on to say that it's a gray area. My question is that after stating that he's an abundant proponent of free speech, if and when the Government passes a law on Spam, will he abide by it?

MS. ARBON: I think discovery is normally done in the legal process.

MR. FELSTEIN: I'm not asking you a question, but -- I understand that, but this is a public forum, and what he says is -- actually will be transcribed and used, but that's another matter. Okay.

I'll answer it, how about -- it's actually for Alan, because my impression of the blacklist is that it's a mob mentality.

MR. HUSEMAN: Let's move on to another question.

MR. MURPHY: I think I have an answer, but I will decline to answer you at this forum.

MR. HUSEMAN: Can we have another question, please? Right here in front.

MR. BAKER: I'm Phillip Pound Baker. I was going to say I'm rarely with Cindy here in that the blacklist people have really got my goat. The gentleman over there has got my goat even more.

The question I was going to ask is whether any

of the blacklists know how often that they list the A route of DNS and the other DNS route. One of the problems that we have on the internet is that there are a lot of really bad people, and it's not just the Spammers, and whenever you have an information collection resource, there will be people who put deliberately false information in, as Cindy mentioned with the Moveon case, but one of the little games that people like to play is let's list the A route on SPEWS, and then the internet will turn off.

Now, you know why that's not going to happen, but you also know that the A route doesn't send a single piece of e-mail.

MR. HAIGHT: So, it doesn't matter.

MR. BAKER: Yes, but it does affect your credibility.

MS. COHN: Well, we were founded by the operator of route server F, so we've never done it.

MR. HAIGHT: It displays the problem of, you know, that there are -- that there is this capability for -- for this sort of thing.

UNIDENTIFIED SPEAKER: (No microphone.)

MR. BAKER: The point is there's a system called the DNS that they have re-used the protocols of the DNS to create this blacklist system, and Paul Vicksy

(phonetic) was the first guy who did it. I think it's a bad use of technology to advertise blacklists, but that's by the by. The point is that the DNS routes are under continuous attack by hackers. Some of them went down a while ago, Paul's didn't, ours didn't. That's because people just want to take out the internet.

So, one of the other things that we see, the little games that people try to try and take out the internet is, let's see what happens when you list the A route on one of these listing services, so they will create bogus claims saying the A route is sending me Spam.

MR. HAIGHT: If I can try and paraphrase, he's saying that black -- if I -- he's saying, if I can try and paraphrase, he's saying how often does the blacklist list this IP address which is obviously not the source of Spam, it could not be, and it's also important to the internet? It's just a --

MR. HUSEMAN: Let's briefly answer this and then move on to another question, please.

MS. ARBON: Let's back up real quick. There are 13, I believe, route servers that answer queries for like calmnet.org, UK, it tells them where the domains are and then they go to the domain system. They are part of how the internet works.

The only way that that would hurt even anything is if it got put into a BGP feed. 99 percent of these lists are being operated on a DNS base that is used by mail server. I think we're the only one that has a BGP feed, and we don't list route servers.

MR. HUSEMAN: Question over here in the front row. I thought there was right there.

Okay, right over here.

MR. BARRETT: Josh Barrett. I really want to echo your comments. I really appreciated Cindy's comments. I thought they really helped give us a vocabulary for things that I didn't have before. From a service provider perspective, I really hone in on -- the two problems for me with blacklists are not that other people may not want to receive mail from us, I think that's okay and they have the right to make that decision.

What the problem is is, like she said, the transparency, not being able to know who it is, not having anyone to talk to, and them often not having the resources to talk to you, and the collateral damage, which I think is the big part of it. It's that -- from a service provider perspective, I can understand their rules and I can set something up where mail that doesn't follow their rules goes off certain IPs, and they might

choose to list those, and I'm okay with that, because I understand their rules and it doesn't follow them, and I have other customers that I can put on IPs that do follow their rules and they shouldn't get listed.

From a service provider perspective, that gets hit by the collateral damage, and at the same time, all these other people are getting hit by it. I think blacklists do have the right to block stuff themselves. They don't have a right to go intentionally damage other companies and try to fix the internet, and I think that's really where the problem of blacklists comes in, is where they're doing all these things besides just stopping them from getting mail from someone they know is sending mail.

MR. HUSEMAN: Does anyone have any response?

Okay, in the back.

MR. LEVINE: Yeah, I'm John Levine from abuse.net, and in case anybody was wondering, does not publish a blacklist.

My question actually picked up on something that Julian said, is that the fundamental economic model of e-mail is based on freeloading, consensual freeloading, that when any -- you know, I have lists of people who have bought my books. I send e-mail to it, which costs me ISP, you know, which is then received by the recipient ISPs out of the charity -- out of the

goodness of their heart, because they think their recipients want it, and I think Moveon is -- I'm Unitarian, so Moveon is wonderful, but -- you know, and Moveon has this large list which is delivered through the charity of the recipient ISP.

So, my question is in this question about responsibility and stuff, how much of a burden -- is it reasonable to put on network providers to deliver mail sent by people with whom they have no contractual or other relationship at all?

MS. COHN: If I can take a shot at that, I actually think that the freedom and openness of the internet is a feature and not a bug, and I think that any attempt to rethink the internet such that it's a little fiefdom of private property where you only get to communicate with someone else with their approval ahead of time will kill something really important that we managed to create with cyberspace.

I think -- I mean, I -- there is certainly a way you could re-imagine the internet that's like that, and -- but I think that you will be missing some of the things that really matter, and frankly, I think ISPs are in the -- you know, they're getting paid to deliver people's mail to them or they're -- you know, they're finding other business models to deliver people's mail to

them, and so the idea that it's charitable for them to do what essentially their customers are paying them to do is something I have a difficult time with.

MR. HUSEMAN: We have an e-mail question we're going to read. The Washington Post reported that the domain registrar of an association of emarketing companies was blacklisted for their association with an organization deemed sympathetic to Spam. Since neither the domain registrar nor the association in question were accused of sending Spam, isn't that using the blacklist to silence critical speech?

Does anyone have a response to that?

MS. COHN: Well, I know that we were recently threatened with blacklisting, because somebody linked --

MR. FELSTEIN: I know what you're talking about. That was my domain --

MR. HUSEMAN: Please sit down. Thank you.

MS. COHN: Yeah, I know that one of the things that we had recently heard was that somebody who actually had a website who was in a fight with some -- you know, there was a Spam/anti-Spam battle, the EFF was going to be blacklisted because their website linked to us, and, you know, again, I think we really have to think carefully about tactics and how far you're willing to go in terms of doing these things and who gets hurt in the

meantime.

MS. ARBON: Can I make a point on what she just --

MR. HUSEMAN: Margie, just one moment, please.

MS. ARBON: One thing I need to make clear, everybody keeps talking about the lists like they're one thing. There's not -- as someone said, there's 400 of them.

The other thing is there are people out there that will send you mail and say, if you don't do X, I will have you put on so and so's blacklist. If doesn't work that way. So, a lot of it's just people getting excited.

MR. HAIGHT: And I have a blacklist of IP addresses that end in dot ten. I mean, you know, there's all kinds of listing criteria, and that's really what defines what a blacklist is, is how those criteria are defined.

UNIDENTIFIED SPEAKER: Is vindictive use of blacklists a problem or no?

MR. HAIGHT: Yeah, it's a problem, one I hope we can overcome, but --

MR. HUSEMAN: Here in the front row.

MR. GELLER: Thank you, Tom Geller from SpamCon Foundation. My question is for Cindy.

In the emarketersamerica case against SPEWS, et al., it seems to me a conflict between two different versions of free speech, one being alleged Spammers saying they have the right to send and so forth, and the other from the blacklists saying they have the right to call them on what the alleged Spammers are doing.

Does the EFF or do you have a position on the rightness or the credibility of that case?

MS. COHN: No. I mean, I've read the complaint, but like most complaints, it's not particularly illuminative of, you know, what's going on, and I have no other information, so I really can't comment about that specific case.

MR. HUSEMAN: Laura Betterly in the back?

MS. BETTERLY: Hi.

MR. HUSEMAN: Wait for the microphone, please.

MS. BETTERLY: I'm the benefit of a lot of press in the last six months, and one thing I have to say, because -- regarding the blacklisting, I was personally blacklisted on SPEWS based on press, not on one complaint, and my upline provider shut off my website based on the complaint -- on that particular thing, although my corporate site has not even sent out one commercial e-mail.

We've found that these kind of things, where

-- if you look at even some of the message boards where guys are being incited to opt-in and then complain and whatnot, and that's a problem, because it actually stops people from legitimately doing business, if anyone could comment on that.

MS. ARBON: We're not SPEWS.

MR. HAIGHT: Yeah, we can't comment on SPEWS.

Does anyone have any response? Okay.

MR. HAIGHT: Certainly I only would list IPs that sent mail.

MR. HUSEMAN: Go to the woman behind you.

MS. BALLY: I'm Karen Bally, also known as Resch Kugal (phonetic) from RCN. We heard earlier from AOL and from Yahoo! and they're using a similar blocking system to SpamCop, which you say is in beta tests and it's completely complaint-driven. You say that SpamCop isn't ready for -- isn't -- it's beta testing.

MR. HAIGHT: I don't say that anymore, no. He -- Scott said that.

MS. BALLY: Right. I haven't read SpamCop in a while, so please forgive me.

MR. RICHTER: Did it come off yesterday?

MS. BALLY: But, so, you get a lot of criticism for the SpamCop blacklist, but AOL and Yahoo! are getting a lot of praise. What are all of your thoughts on this?

I mean, we have -- we hear from the legal part that SpamCop might not necessarily be legal. So, how does this apply to AOL and Yahoo! as well?

MR. HAIGHT: Yeah, that's exactly what I'm worried about, is that anything that's applied to those of us who are a little aggressive in our blocking is going to then be applied, you know, successively to less and less aggressive black -- filtering in general, I mean blacklists is just one kind of filtering, and eventually you get to a point where filtering all is illegal.

MR. HUSEMAN: Stuart Ingis?

MR. INGIS: I think the praise comes from the fact that in many ways filters and blacklists are effective. I think the criticism comes from the fact that there are excesses and where there are legitimate communications that are being blocked, and I think that that probably is the issue that needs to really be the focus going forward.

MR. HAIGHT: Yeah, but we have to recognize that nobody's perfect, that there are going to be mistakes.

MS. ARBON: And on the flip side, there is excesses with bulk mailers where they don't send at the same -- they will try to send at the same rate to a huge

ISP as a small ISP, so --

MR. HUSEMAN: Trevor?

MR. HUGHES: Sure, you know, my response to that is that I think the false positive problem exists throughout ISPs using proprietary filters and ISPs using blacklists. It exists in both places, and we're concerned about it in both places.

One of the differences, the key differences that we see, is that the major ISPs with proprietary filters are engaging in a debate, in a discussion, because they recognize the false positives are a problem for their subscribers, that if their subscribers are not getting messages that they otherwise want to receive, that that's a customer service issue for them.

Blacklists have no similar skin in the game, and the -- one of the significant differences that we see is that we -- okay.

MR. HUSEMAN: One more response and then one more question.

MS. ARBON: I would beg to differ, because I would say at least four times a week I get e-mail from bulk mailers, service bureaus wanting our help to understand what we consider to be best practices and how they could apply it, and we are more than happy to discuss that with anybody, any time.

MR. HAIGHT: We're very concerned about these problems.

MR. HUSEMAN: Behind you, standing up, that would be the last question.

MR. BROWER: I'm Adam Brower, citizen of the United States. I have an interesting question, a paradox that just occurred to me. It seems to me that part of the meat of this issue is the associated text records with listed IP addresses. In other words, might an operator of a block list immunize himself against putative claims of damage by supplying no explanatory text record and simply listing an IP address? I address this to all the panelists.

MS. ARBON: Most of our lists don't have text records anymore. It's more of a function of the fact that when you have a 25 megabyte zone in and of itself, adding text records is a little bit ridiculous.

MR. HAIGHT: And that won't protect you, because the recipient site is blocking -- is going to implicate you eventually.

MS. ARBON: And the bounce message we recommend will say specifically why someone is listed.

MR. BROWER: May I clarify, because I wasn't really clear in my comment or question.

MR. HUSEMAN: You have ten seconds.

MR. BROWER: Okay, there are several block lists that maintain also explanatory sites, explaining to the blocked individual why his mail may or may not have been bounced. Without associated explanations, would part of this putative problem of damage disappear?

MS. COHN: So, less transparency would make it even better? Yeah, I would have a real hard time with that.

MS. ARBON: No, we want people to come to us and ask us why they're listed so we can tell them how to get off.

MR. HUSEMAN: Thank you very much. We're out of time. We will start promptly back at 1:45 p.m. Thank you.

(Whereupon, a lunch recess was taken.)

AFTERNOON SESSION

MR. SALSBURG: Okay, we are going to get started. So, could the people please come on in and take a seat?

We have a couple of really quick announcements before we get started on the best practices panel. The first one is, does everybody know the best practice regarding cell phone use? We heard a few phones ringing earlier today and yesterday, and the announcement that we have is if self-regulation doesn't work, we will be forced to call Congress, so please turn off cell phones.

For much of the last day and a half, we've focused on worst practices, things like harvesting, dictionary attacks, falsity in Spam. We've seen the dark side. Now we're going to see the light side.

And to help me with this, we have a really distinguished set of panelists. On my far right is Jason Catlett. He's the President and Founder of JunkBusters.

Next to Jason is Ted Gavin of the SpamCon Foundation.

On my immediate right is Tim Lordan, who is the Staff Director of the Internet Education Foundation.

On my left is Rebecca Lieb. Rebecca is the Executive Editor of internet.com's Interactive Marketing Channel.

To her left is Anna Zornosa, and Anna is the CEO of an e-mailer called Topica.

On her left is Michael Mayor. Michael is the President of another e-mailer, Netcreations.

And at the end of the panel on my far left is Ben Isaacson of the Isaacson Group, and he is a consultant to e-mail marketers.

So, what are we here to talk about? Well, our goal here today is to identify best practices, not okay practices or pretty good practices, but really to find what are those practices that both consumers and industry members can engage in that will help solve the problem that we've been talking about, which is a volume of e-mail that is threatening to burst the system.

So, let's start with just identifying some best practices for the panel. As with the other panels, if any of the panelists want to respond to comments made by another panelist, please put up your name tent, and I'll let you have your -- say your piece. If any of the members of the audience want to ask a question, please hold it until the question period at the -- towards the end of the panel. And if anybody on the conference call line wants to ask a question, you can fax it to spamquestions@ftc.gov.

So, why don't we get started by first talking

about best practices for consumers.

Jason Catlett, I am a consumer who's about to open a new e-mail account. I've heard about something called Spam, and I don't want to receive it. In fact, the only reason that I want to have an e-mail account is to receive and send personal e-mail. I don't want to have anything to do with any commercial e-mail.

What should I do when I'm establishing my e-mail account to ensure I don't get Spam?

MR. CATLETT: Okay, my answer is going to be quite long and complicated, and I'd first like to comment on the fact that it has to be like that, particularly with the name best practices, which suggests sort of this is business as usual and the way things are and the way it should be.

You shouldn't have to follow the advice I'm about to give you. If we had a proper public policy in place about Spam, these measures would not be necessary, and it's going to sound like I'm describing a state of siege because of the threats that you're trying to counter and the measures that you're taking, and that's what it's -- that's unfortunately the way it is.

So, I'm assuming you are, as you said, a consumer, and you can buy a new e-mail address. There are two things to consider here in the e-mail address.

There's the bit before the "at" sign and there's the bit after the "at" sign, and you have some freedom in choosing those, too. You want to try to avoid dictionary attacks, which we heard about yesterday, with -- if you choose a name like john42@aol.com, well, it's probably taken, but even if you could get it, you would probably get a lot of Spam even if you did nothing to reveal your e-mail address to the public. So, the dictionary attacks would find out that that address is valid and would -- you would get Spam from it.

MR. SALSBURG: Are you less likely to be the victim of a dictionary attack if your e-mail address begins with a Z rather than an A?

MR. CATLETT: That's -- I believe that effect would be true, because a lot of junk e-mail lists are purchased sort of alphabetically, and a lot of Spamming campaigns are cut off by an ISP in mid -- throughout the middle of it. So, if you choose -- if the first letter of your e-mail is a Z, you are probably likely to get less Spam. If you're very high in the alphabet, I think you may see a disproportionate increase.

MR. SALSBURG: Do the number of characters on the left side of the "at" symbol affect your vulnerability to a dictionary attack?

MR. CATLETT: Yes, but it depends on your

choice of characters. Maybe I should give you my ideas on what those bits on the left should be.

It should not be a common name, first name or last name or combination thereof, because Spammers look at these lists such as ted@aol.com, and they say, well, let's try ted@earthlink.net, ted@yahoo.com and so forth. So, something that exists elsewhere, you should not choose.

Some people say, well, should I then get the cat to walk across the keyboard of my PC and use the 16 or 17 letters there as my e-mail address? Well, that's probably pretty random, but the problem with that is if you want to tell a -- your grandmother your e-mail address and you're speaking over the phone, it's going to sound like alphabet soup, and she is going to have some difficulty with it, or if you're in a noisy bar or if you want to scratch it down on the back of a napkin, it's not very intelligible.

So, one trick that I've recommended is using something like an acronym. For example, the letters TBONTB are not obvious, but if you remember Hamlet, "To be or not to be," that's fairly simple. Putting in numbers also helps, although if you want to speak the name in a bar, then a lot of numbers are easily confused, like the digit two or the letter -- letters T-O. Zeroes

get confused with Os; ones get confused with Ls. So, I would actually recommend if you are using numbers, avoid the binary numbers, zero, one, two, four, eight, and go for the nonbinary numbers, three, five, six, seven, nine.

The -- and longer is better. Of course, longer is much more cumbersome and more difficult to remember, but if you choose a favorite line of poetry or a catch slogan or something like that, you can devise something unique that is unlikely to be guessed by a dictionary attack.

MR. SALSBURG: Or I imagine something like -- if your name is long enough, your name spelled backwards even, you can let somebody know.

MR. CATLETT: Yeah, that would be good. I hope no dictionary Spammers are listening to that one. I think they're unlikely to try that. I mean, that shows you we're really dealing with an arms race here where counter-measures are being met by counter-counter-measures.

MR. SALSBURG: In addition to the dictionary attacks, if I were to open an e-mail account and only use it for personal e-mail, are there any other sorts of methods that my e-mail address could be gotten by a Spammer?

MR. CATLETT: Well, principally the e-mail you

send to your wife could be intercepted by the Spammer in transit, but it's extremely unlikely. It's not a convenient or an economical attack for them. So -- actually, go ahead, Ted.

MR. GAVIN: There is a recent case that has caused much controversy in the public. A commercial white list provider had in its privacy policy that if you send e-mail to somebody who is our customer, it goes through our system, it comes back and says, hey, you're sending e-mail to Bob, and Bob's using our service, just click here and type in what you see, and you can send your e-mail to Bob forever. This service then took the addresses of people who were corresponding with their customers and sent them unsolicited commercial advertisement for their service, saying, hey, you won't get Spam if you use our service.

Now, the ethical questions notwithstanding, it was, in fact, in their privacy policy that they were going to do this. I look at this from a few perspectives.

My day job is very heavily rooted in business management, consulting for distressed companies, so I understand best practices like ISO 9000, which is quality, and you can be quality certified and say that our quality practice is we're going to pour sugar in the

gas tanks of our customers because we don't like them. You can get certified as long as you can do that consistently. So, having a privacy policy that says bad things or says we're going to do things that probably aren't going to be very popular in the public is not necessarily a cure-all.

So, to that degree of if we're just going to send e-mail, you know, if I open my new account and I only send to my friends, my friend may subscribe to a commercial service that I then have to interact with even though they are basically my friend's proxy, which gives them access to my e-mail address, which they can then use or sell or it gets scraped or any number of other things, which now takes control of that address completely out of my hand, and I had no idea that that would ever happen, because all I wanted to do was send e-mail to Grandma.

MR. SALSBURG: So, then, there is virtually no way to protect yourself here?

MR. CATLETT: Well, there's -- the only way to get absolute privacy and security in e-mail is to turn off your computer and disconnect it from the power supply. Beyond that, it's really a matter of controlling the level of exposure to the different attacks, and I think -- I don't think any major ISP currently would pull the kind of dirty tactics that Ted describes,

although I'm sure it is a risk, and if you e-mail a lot of people, then obviously there's more opportunity for harvesting that address.

MR. SALSBURG: The way Ted described it, the risk, though, is something that you couldn't control as the consumer.

MR. CATLETT: Correct, because -- well, under U.S. law. You could argue under many -- under the privacy laws of many other countries that that was unfair collection and take action against the party that harvested it, but we don't have such a right in the United States.

MR. SALSBURG: Let's say the consumer is the more typical consumer, doesn't just want to use it for --

MR. CATLETT: Okay, actually, we didn't do the right-hand side of the "at" sign. Should I do that?

MR. SALSBURG: Sure, do the right-hand side.

MR. CATLETT: Should I give advice on that?

You do have a choice of what goes on the right-hand side based on the ISP that you go to, and I'm afraid the bad news is that the large ISPs tend to attract more Spam, not because they're lax on Spammers but because -- well, I mean, it's the same reason as bank robbers rob banks, it's because that's where the

money is, and Spammers harvest addresses from large ISPs because that's where most customers are. So, your Yahoo!, your AOL, your Earthlink and so forth is more likely to be the subject of a dictionary attack than others.

Now, you can still have your internet service from such a company but not use an e-mail address with them. You can register your own domain name and then have it forwarded, but that actually brings up risks of its own, because many registrars will provide in certain circumstances e-mail addresses to other parties, and particularly you would not want to forward, for example, web master to your own account, because that is probably the number one Spam magnet in the world.

So, if you have a choice of where to register, if you're registering your own, the ideal top-level domain to get is dot gov, but you would have to start a government department or institution in order to obtain that, which is very burdensome on consumers. Probably dot com is one of the worst, and some of the two-letter exotic countries are probably a better choice.

There's lots of competition in the registrar business now. You can register many choices of countries, from lots of different sources, and I've heard reports that say a registrar in Germany has a more

restrictive policy on disclosing the existence of the domain's contact detail than, for example, some of the major vendors that have a larger market share.

MR. SALSBURG: Are harvesting programs less likely to harvest a domain that has a two-letter country code?

MR. CATLETT: I think they'll still get it anyway. I don't think it's -- they see the "at" sign, and they recognize the country code. I mean, I know Spammers -- some Spammers certainly do have a policy of throwing away dot gov to avoid, for example, Spamming a Commissioner of the Federal Trade Commission, but I don't know if they're more likely to Spam -- we're assuming here that the address is not put up on a web page or maybe that's going to be your next question. So, to summarize on what's on the right-hand side of the domain, the more obscure is less likely to be the subject of dictionary attack and therefore more protected.

MR. SALSBURG: Okay, so let's move on to the consumer who also, in addition to wanting to send personal and receive personal e-mail wants to engage in some commerce, wants to visit the travel site, subscribe to a newspaper, you know, an online newspaper, that sort of thing. What additional steps should that consumer take to reduce the risk of being Spammed?

MR. CATLETT: So, the common practice here is to reserve your real e-mail address or some other alias for personal correspondence and to have a disposable e-mail address of some kind for the purpose of signing up for a newsletter or giving to an airline when you make an online reservation, and there are various ways of getting disposable e-mail addresses.

A common one is using a web-based e-mail service, such as Yahoo! mail, Hotmail, and there are many, many alternatives there. That has a bit of a difficulty that they tend to expire after a certain period of time, which may or may not be a problem. Perhaps you want to be able to check for e-mail saying your reservation is being changed and you're now flying out at 6:50 p.m. instead of 6:40 p.m. So, the time expiring may not be a problem if you go on vacation.

It's also possible to get purpose-built disposable e-mail addresses with a time destruction feature on them that say after seven e-mails to this address, it stops forwarding. There are -- there's the option of many ISPs, if you have a mid to high tier internet plan with them, will offer you several addresses, and you can use some of them for the purpose of those commercial transactions and revoke them if they start to be the source of more Spam.

Of course, that burdens you with the job of looking at the headers to see which e-mail address it was sent to and then maintaining them, but it's better than having to abandon your real principal e-mail address, which often, frequently occurs.

MR. SALSBURG: What happens if rather than to start again with a new e-mail address, you have an e-mail address, you have given it out to all your friends and family, your business colleagues, and it is inundated with Spam? How do you clean it up? Is it possible to make that e-mail address a good address again that you can feel safe going to your inbox and not having to review a boat load of Spam every morning?

MR. CATLETT: I don't think it's possible. It's -- I mean, you could try getting off these e-mail lists, and in some cases you can reduce the volume a bit. It depends on how your address was contaminated by the Spam, but in general, it's not possible.

MR. GAVIN: Dan, I think there are new technologies out there that you can now forward your e-mail address on to one of these new kind of inboxes that has challenge response systems, so that you upload your approved sender list, and any other e-mail won't get into your inbox as a result, so you can continue the legacy old e-mail address, and it just forwards on to a

box that only has a challenge response system set up.

MR. SALSBURG: So, did you want to --

MR. CATLETT: That's true, and my answer was omitting the whole field of filtering systems, which you can add to -- add to your e-mail address, but your e-mail address is still going to get the Spam. It may be filtered by someone else. And I should say, some of these systems are becoming fairly easy to use by changing the POP settings and putting basically what's a bump in the cord to your delivery. You can get filtering added on, but it's still a filtering solution, even though it doesn't come to your PC, it may be filtered before it gets to the PC, and with filtering come the inevitable false positive errors there, so...

MR. SALSBURG: The precise type of filter -- Ben Isaacson, you're describing is the challenge?

MR. ISAACSON: It is a -- correct me if I'm wrong, the e-mail comes in, and if the e-mail isn't from somebody on your address book, there's a question asked, you know, who are you? Give some information. And if it's Spam, it's automated, and there will be no response, and it won't get through.

MR. CATLETT: Well, actually, that's not true. It may not be Spam. It may be, for example, the airline mailing you your reservation number and confirmation, and

they're sure as hell not going to respond. It's not Spam.

MR. ISAACSON: That's why you made the false positives comment.

MR. CATLETT: Right, yeah.

MR. GAVIN: And one additional problem with that is you don't always know from what address something that is critical to you is going to be sent, you know, you take some of the larger travel ticket clearing houses, they may have hundreds of mail servers that send from hundreds of IPs and hundreds of identities. I have virtually no way of white listing those after forwarding to an e-mail box, and they're not going to -- you know, they're not going to call me and say, well, we sent you your ticket, and they are not getting an undeliverable. There is a message saying, you know, click here and type in what you see in the picture, and that's not going to be recognized systemically. So, not getting the airline ticket may be almost as bad as having deleted it mistakenly because it was under the deluge of Spam.

MR. SALSBURG: So, far from a perfect solution.

MR. GAVIN: I would agree, it is far from a perfect solution.

MR. SALSBURG: Jason, what is munging (phonetic), and is it an effective strategy for

consumers?

MR. CATLETT: Ted, do you want to take that?

MR. GAVIN: Sure, I guess I will speak to that. Munging is the practice of altering how a person's e-mail address appears in a given medium that is readable by humans and intended not to be readable by harvesters, the intent being if I change my address so it is no longer alphanumeric string at alphanumeric string dot something, the bots (phonetic), the e-mail address harvesting programs will not be able to automatically get that.

We heard discussion yesterday about different methods through which munging was more or less effective given different types of harvesting technology. There are a few problems with munging. First, it's considered incredibly rude if you munge your e-mail address and you're participating in e-mail correspondence. It is generally much more widely used in usenet posts and in public forums, such as web sites or online discussion groups.

You know, if I send an e-mail to you, Dan, and I've physically altered my e-mail address, so instead of being tedgavin@example.com, it's tednospam___ @example.com, and somewhere in the body, I say, "Remove nospam___ to reply," you're probably not going to reply too many times, because there's far too much effort

involved in the process than is really warranted.

The problem that we've seen technologically over the past five or six or more years is that as -- you know, munging is one of those anti-Spam techniques that is basically building a broader or higher wall to protect yourself from the flood of Spam, and what that does is it promotes people to design software which is basically more effective, stronger battering rams to get down the walls.

There are munging programs that know how to decipher different types or there are harvesting programs that know how to decipher different types of munging and look for cues that are commonly used and automatically filter them out.

So, while we heard yesterday that physically spelling out all the characteristics of addresses, like spelling out A-T for "at" or D-O-T for "dot" have varying degrees of effectiveness that tend to be more effective than inserting various alphanumerics into the e-mail address, nothing is perfect and, you know, this is, as Jason said, an arms race.

Everything is always responsive. You're going to munge because you got Spammed. Somebody is going to see that affecting their ability to harvest and will come up with a technology to work around that, and then we go

to another step of reactive steps.

MR. SALSBURG: So, let's say I have an anti-Spam program that I want to market. I very well might Spam people based on the harvest program that collected just the names of those people that munged.

MR. CATLETT: Those sorts of conspiracy theories are always leveled against anti-virus companies who are accused of making up viruses so that people are forced to upgrade. It's a cute theory, but I simply don't think it's true. There's enough Spammers and enough virus writers there to explain it without any conspiracy.

MR. SALSBURG: Tim Lordan, let's say that as a parent of young children, my main problem with Spam is the pornographic images that automatically appear when I open certain messages. Is there anything that I can do to prevent this?

MR. LORDAN: Well, when it comes to young children, what you really need to do when it comes to porn Spam, on our getnetwise.org website, we say -- and you've heard this before, parents -- it says, take the computer, put it in a room, a common room like the den or something, get a big screen so you can see what your kids are doing, and lo and behold, the porn Spam comes up when you're checking your e-mail, and it's harsh, the kids are

terrified.

One thing you can do, and you actually mentioned it, is actually converting the e-mail client to display only text. Now, what you've done is you've downgraded the richness of the medium from images to text, certainly not for porn, but for other things that are more worthwhile.

So, you can do that, but for kids, you know, my basic message for kids is, depending on their age group -- I mean, a 15-year-old is vastly different than a 10-year-old. For kids of the younger ages, under 11 or something, what you want to do is set up an e-mail account and have an address book of their aunts, their uncles, their cousins, their sisters, their pen pals, et cetera, and let them only accept e-mail from those people.

You know, if a new friend they met at the park is trying to e-mail them, you know, there's ways you can add that to the list, but that's a really good strategy.

MR. SALSBURG: And Jason Catlett, assuming it's my e-mail account, not my children, I can't really limit the people that are sending e-mail, if I want to get rid of the so-called sporn, can I -- how easy is it to adjust my e-mail program to convert HTML code coming in just to plain text?

MR. CATLETT: Well, it depends on your e-mail handler. Some allow it. Others don't. I personally don't use Microsoft products as a conscientious objector, but I'm told that in Outlook or whatever their product's called, it's actually not possible to disable the HTML rendering, and in the preview perhaps also, there's a whole another privacy issue there with the web bugs rendering the -- sending back information that the e-mail has been delivered.

So, the -- without giving details on particular products, some products don't have good defaults. You know, I think by default, there should be no rendering of HTML graphic e-mail because of the privacy impact that it has, but some of them not only have bad defaults but don't even have the opportunity to turn off some threats.

MR. LORDAN: Well, since you mentioned the kids online issue and the parents trying to protect their kids from porn or whatever, we're now talking about Spam, and Jason was right, it is long and complicated, and I don't even think you've exhausted your -- you have come close to exhausting your knowledge on setting up an e-mail account, and I think compare what a parent will do to keep their kids safe online. Parents will do extraordinary things to protect their kids, you know,

stories of women lifting cars and, you know, doing anything to protect their kids in danger, and people and parents are willing to do a lot more to protect their kids from Spam. They're willing to listen to -- which is not only a quarter of the way there -- all of the things that they can do to protect their kids.

What is the average user going to do? What should we ask the average user to do to protect himself from -- everybody is really upset about Spam, but it's really an annoyance. What are they willing to do? It isn't protecting their kids from sexually explicit material in most cases, and it isn't protecting them from sexual predators.

Parents will download software tools, they'll figure out the blocking lists and everything, they'll do -- they'll take extraordinary steps to control their kids' online experience when it comes to predators and porn. When it comes to the average user dealing with the annoyance of e-mail, how much are we asking them to do? What is too much?

I think the Federal Trade Commission has it right, the ftc.gov/spam site has some really simple times, some good tips, and they're going to change, you know, it is an arms race, and things are going to change. Our tips are going to change, but I think you can only

ask so much of consumers, and maybe not ask anymore.

MR. CATLETT: Sure. I mean, consumers have a certain amount of effort that they're willing to put into maintaining a service before they abandon it, and we are heading from 20, 30, 40, 50, 60 percent, there will be a tipping point where the majority of consumers consider it too much effort and will abandon e-mail, and we will have had an enormous economic tragedy, because the gains of the late nineties in technology and economic gains will be jettisoned because the medium has been spoiled.

MR. SALSBURG: Ted, did you have a comment?

MR. GAVIN: I do. I have a few comments on both points. Ironically, it may actually be more effective in protecting children from inappropriate content to give them their own e-mail account and apply white listing. Parents should have some idea of who is sending mail to their kids, and that is a perfect way.

I think the efforts of internet service providers, and I won't name names, but they're a large one in Virginia and they're nice enough to tell me when I've got mail, you know, the ability that they give parents to say, children have this type of account, and they can't get e-mail from the outside, or they have this type of e-mail account, and they can only receive e-mail from people whom I specify, is very effective.

It can be even more complicated if you're allowing your child to share the parents' e-mail account, because you may not want the child seeing legitimate e-mail that the parent gets. So, at what point do you -- you know, do you draw that line?

To what Jason was just saying about when e-mail breaks, e-mail was and in many ways still is the ultimate killer app. It passes the grandmother test. You know, if I can explain to my grandmother how I can send me an e-mail, there is no stopping her. She has just discovered a whole new realm of the world, and it's valuable.

However, if I have to explain to my grandmother that if she wants to keep herself from getting Spammed or my child, setting up an address at college from getting -- if he wants to keep himself from getting Spammed, to use nonbinary numbers rather than binary numbers in the address, I may have just gotten to the point where they glaze over and say, you know what, this just isn't going to happen, and that does threaten the viability of e-mail as a mechanism for communications and commerce.

MR. SALSBURG: Tim Lordan of the Internet Education Foundation, what do we do about that? How do you take technophobes who are using the medium and want to protect themselves and give them the tools they need

to protect themselves?

MR. LORDAN: Well, I think the Federal Trade Commission educational resources, the consumer educational resources coming out to the appropriate level, they don't attack them with tech know-jargon. I have heard terms here today that I have never even heard today. Am I the only one? And this is a really sophisticated audience.

What you need to do is have really -- I mean, how many data elements can a consumer remember? What is it, five, seven? Seven data elements? And you need to be able to hit those top seven elements. We can't ask them to do any extraordinary measures, because I don't know if anybody saw the Pew (phonetic) internet study that was done about a month ago. Forty-three percent of people aren't online, and a lot of them proudly proclaim, I'm not online, like it's a badge of honor, and I think, what are we talking about here today?

And I'll stop talking, but what are we talking about? Are we talking about maintaining the status quo with regard to e-mail clients, and here's their e-mail client, but are we talking about, you know, the future of personal communications and the evolution of the internet?

People are just going to -- at a certain

threshold, Jason's right, they are just going to abandon it. They are going to abandon e-mail, and maybe they will move to instant messaging or some other type of form of personal communication, but I think what I've heard today -- and I've been out a lot this week, I apologize, I haven't made all the panels -- but I see more of talking about maintaining the status quo rather than addressing the evolution of the internet, particularly e-mail and other types of personal communications, and I think that's really a huge challenge.

MR. SALSBURG: Jason, parting shots on best practices for consumers before we move on?

MR. CATLETT: Well, I could go on for hours, but I'd actually just point you to the pages on our website that have similar tips to the one that I've given today, but I think it's improper to blame the dumb consumer for not spending hours trying to figure out how to do this kind of self-defense.

The medium has to be protected, and we should have a law that says Spamming is illegal, and there should be a private right of action by the consumer who is Spammed against the Spammer directly. Now, none of those laws are on offer at the moment before Congress, but they sure as hell should be I think, and --

MR. SALSBURG: Well, we will be discussing

various legislative proposals on the panel tomorrow.

MR. CATLETT: Um-hum.

MR. SALSBURG: I guess actually, Tim, I'm going to give you a parting shot on best practices for consumers, if you could briefly describe, what do you have on the getnetwise website that would help consumers.

MR. LORDAN: Well, we expanded -- getnetwise was a kids online safety campaign. We are starting to expand the repertoire into user empowerment with regard to Spam, privacy, security. With regard to that, I would, you know, welcome people to visit Jason's -- I think Jason's tips, the Federal Trade Commission tips, our tips, at spam.getnetwise.org, are all pretty much similar, but, you know, at a certain point, you are going to realize that people only do so much, and 43 percent of people aren't online, and some are proud of it.

MR. SALSBURG: Ben?

MR. ISAACSON: Before we move on, I think it's kind of a key point, we've been talking about this the last couple days, and it hasn't been addressed enough, the fact that I think it's up to the internet service providers to help educate consumers on what is Spam and what they can do to get off these lists and try and eliminate the amount of Spam that's being driven.

I think that there's, you know, the Yahoo!

sweep stakes and some of the other efforts, they don't do enough justice to the fact that consumers just do not know what is coming from some of the people on my right here and what is coming from the egregious actors.

So, strong, consensual education campaign from all the major ISPs working together would be something of great benefit to consumers.

MR. SALSBURG: So, consumers can't do it alone. They need the ISPs and all the players to -- to do something about the Spam problem?

MR. ISAACSON: I think so. Every time they open their inbox, they should at least get some information about how to stop the bad actors.

MR. SALSBURG: Well, let's turn to the role that e-mailers themselves can play in curtailing the Spam problem. We're going to look at best practices in four areas. The first one is disclosures and the from or subject line. The second one is the obtaining permission for sending e-mail. The third one is unsubscribing from e-mail lists. And finally, fourth, we'll look at the practice called e-mail appending.

Let's start with disclosures in from or subject lines. In a study that came out earlier this week in the Division of Marketing Practices at the FTC, we found that 44 percent of the Spam that we looked at contained false

information in either the from or subject line.

Ben Isaacson, you helped create in your work at the Association of Interactive Market's Council of Responsible E-mailers, you helped create their Best Practices Guide. Is there ever a circumstance where an e-mailer should falsify a from or subject line?

MR. ISAACSON: Well, I think we had talked about this in other -- in the falsification session yesterday where there are circumstances where the brand identity of the sender, the content of the message, might be different from the actual sender. I wouldn't call that falsification. So, except from those situations, I don't think there are -- there are any good examples of falsification of a from field or a sender field.

MR. SALSBURG: So, if an e-mailer is sending out commercial e-mail on behalf of a client, the from line should list the client's name?

MR. ISAACSON: Well, it can list either the list owner's name, could certainly list the service provider's name, but I don't consider that falsification. That's simply who is sending the e-mail. It should be responsive and identifiable and there should be an accountable company or service at the other end of that from address.

MR. SALSBURG: Okay. Any other comments on

that or -- okay, the same FTC study found that only 2 percent of the messages looked at contained an ADV label in the subject line. Is this a practice that should be a best practice? Should e-mail that's commercial in nature include an ADV label?

Michael Mayor?

MR. MAYOR: Absolutely not. I think it's a ridiculous law. I think most of the laws that we have that are ADV are state by state and, you know, before we get too deep into the different types of laws there are, I think it's a terrible misconception to think that e-mailers or list managers have all this kind of information on their list members. We don't know all the time what state they're in or what country they're in.

When we started our company in 1997, we just asked for their e-mail address, because we were asking them what they wanted to receive. What more do we need to know? And so, you know, now we're getting deeper and deeper, and we need to ask all of these questions so we can guide ourselves around the law --

MR. SALSBURG: If this were a Federal requirement, would that solve your problem with it?

MR. MAYOR: No, absolutely not. What does it do to stop Spam? ADV does nothing. Spammers may or may not use ADV. Why should I use ADV? They know that

they're getting advertisements from me.

MR. SALSBURG: Ted?

MR. GAVIN: There are a lot of risks to the use of ADV and especially a legislated use of ADV, because as we've heard about collateral damage and false positives, if I decide as a consumer or if my ISP decides, acting on my behalf, to filter traffic marked ADV, there's a fairly good chance that I'm going to stop getting my online credit card bill or my online phone bill. Without any type of way for the sender to assert, this is who I am, this is what I'm doing, and this is wanted, rather than just some more ADV-classed mail, you break the system.

MR. MAYOR: The thing that I would add to that is that most of the laws are written that if you are sending unsolicited e-mail, you need to use ADV. Well, I'm not sending unsolicited e-mail, and if I do send it ADV, I'm sticking my hand up and saying, hey, I'm a Spammer, and I think that's ridiculous.

MR. CATLETT: Could I add, almost nobody thinks ADV is a good idea. Certainly consumer groups generally don't think it's a good idea. The EPIC, for example, which is also concerned with free speech, doesn't like the compulsory labeling. It -- people sometimes say, well, it makes it easy to filter, but in fact, that doesn't practically work, and filtering is not a

sustainable solution to Spam anyway. So, I think everyone thinks that this compulsory labeling is a bad idea.

MR. SALSBURG: Rebecca Lieb from internet.com's Interactive Marketing Channel, do you think it's a good idea?

MS. LIEB: I think it's a terrible idea, and I think it's not a terribly well-defined idea. There are all kinds of commercial e-mail. My company publishes double-confirmed opt-in newsletters. The vast majority of them are free, and we're advertising supported. Because our e-mail originates from a corporation and there are advertisements in those e-mails, would that then require us, for example, to put ADV on our newsletters? You know, if that were the case, I would argue that The New York Times would have to be called New York Times ADV, it's effectively the same situation, and that font would have to be as big as the headline font.

By the same token, I don't know that this would apply to my brokerage statement or my bank account statements, which are also arguably commercial e-mail, they come from commercial entities. They couldn't be more personalized or more opt-in. Are they advertisements?

MR. SALSBURG: Would a more complex labeling

system solve some of these issues?

MS. LIEB: I think a more complex labeling scheme would be more complex.

MR. SALSBURG: Ted?

MR. GAVIN: You know, one of the problems with calling things -- you know, calling the problem unsolicited commercial problem is that it costs just as much to receive unsolicited bulk noncommercial e-mail, and so saying, okay, the problem will be solved if only we put ADV, means that, oh, somebody who's running for the Governor of California, for example, can send unsolicited e-mail to people in Toronto in huge numbers, and that passes by without any type of labeling.

So, again, we hit that slippery slope of trying to define and solve the problem based solely on content, which, you know, it doesn't cost the recipient or the ISP or the sender any more to deal with a content-based list gone awry than it does a consent -- you know, if it's commercial or if it's noncommercial, it's going to have the same damage.

MR. SALSBURG: Michael Mayor, at Netcreations, you send e-mail on behalf of clients. Is that right?

MR. MAYOR: Um-hum, correct.

MR. SALSBURG: And the question I have is, should an e-mailer such as yourself do any checking to

make sure that the subject line matches the content of the message before you send it out?

MR. MAYOR: Absolutely, absolutely. I mean, we have very clearly asked the list member what they want to receive, and let me say this first. I think the from line and the subject line are the meat and potatoes of direct marketing, and you really need to be clear about who you are in the from line, and I agree with Ben that it should be either your brand or the list owner in certain cases. I can't think of a third case that's okay. Maybe there is one.

But then the subject line is -- that's your direct marketing power, and deception does not work in e-mail. You need to be very clear, and you need to say who you are and what you're offering, and we do check for that, absolutely.

MR. SALSBURG: Anna Zornosa?

MS. ZORNOSA: Yes, I would agree completely that there's no room for deception in the case of e-mail. You know, it's -- what we find in our case is we've got, you know, thousands of customers using our products, not just for marketing but also for communications, and when -- you know, from nonprofits to discussion groups to large marketers to large membership organizations, and it does become impossible for us to verify their subject

lines.

But I'll tell you that, you know, we do an awful lot in the area of education, and they also see a lot. You know, today, a legitimate mailer who does in any way start to deceive on the contents, we'll see that immediately. You know, we can actually see the patterns as they relate to unsubscribes and as they relate to complaints when even a legitimate mailer starts to veer in the direction of becoming confusing to the people that they intend to reach.

MR. SALSBURG: If you were to receive complaints against a client for falsifying a subject line, what would you do with the client?

MS. ZORNOSA: The -- we would -- if the complaints were of that degree, we would definitely fire that customer. The -- of course, you're talking about a gray area, you know, falsifying a subject line. The first punishment that that mailer will get is if the subject line is confusing to the person who is receiving it, it will immediately pummel their open rates. You know, we've actually started to counsel our customers not to, you know, go in the direction so much of talking about what's in the subject as opposed to saying, you know, publishers lunch, Monday, the 16th, because the more consistent identification they can do with an

audience who understands and trusts them, the better they are going to get in terms of results.

MR. SALSBURG: How do you check an open rate? Is that based on the pixels that are included in the messages?

MS. ZORNOSA: You can only see an open rate, of course, if the message is not text. So, you're talking about HTML and multi-pipeline, which for the most part do not encompass 100 percent of the messages that a customer receives. So, an open rate on that portion of the list that can be seen is, you know, in most cases extrapolated to the entirety of the list. Both HTML and multi-pipeline, it's very easy for the list owner to see their open rates. It's very easy for us to see it on their behalf and to, you know, to be able to interpret it.

MR. SALSBURG: If I have my e-mail program set to preview e-mail and I see the first few lines of every message, is that considered opened?

MS. ZORNOSA: In our system, it is not. In many systems, it depends also where the pixel is placed in the newsletter themselves.

Rebecca, is that common?

MS. LIEB: In some cases, it also depends on what e-mail client you're using to preview. In some

cases yes; in some cases no.

MR. SALSBURG: Okay, well, let's move on to probably the real meat and potatoes of best practices with e-mail marketers, and that's obtaining permission for sending e-mail.

Rebecca Lieb, what's the difference between permission-based and nonpermission-based marketing?

MS. LIEB: Spam and not Spam. This is an interesting subject, and I -- it's one I'm very glad that we're getting into here, because lots of references have been made over the past two days to opt-in and opt-out, and there are more subtle gradations along that chain, and I've identified five, and over lunch, Mike told me he had identified four, so even marketers aren't quite in accordance on what they are, nor the language that is used to describe them.

So, when I -- I will -- my descriptions of these are going to be more important than what I call them. Some people say, well, only Spammers call it double-opt-in, and if it's really double-opt-in, you have to say it's confirmed opt-in if you're legitimate, semantics. I suppose people are eventually going to agree on the terminology. What's important is to understand what the various options are and what they mean to both users and to e-mailers.

Legitimate marketers want or should want to do the best thing. You know, Spam is obviously infuriating a lot of people, and that's why we're all here. It is the goal of marketers not only to make their audience like their products and themselves in order to sell or to effect transactions. I would also posit that one of the first tasks of marketers is not to make that same audience hate them, because then, you know, working towards like or love is going to be a much more difficult task.

I'd also like to preface this by saying that e-mail is a very low-cost medium. It's not absolutely free, but it's close to it, and the barrier to entry is very, very low. You know, just as I'm a journalist, anybody can go on the web and become a journalist and publish their writing. It doesn't mean it's going to be as good as mine is, you know, with 25 years of experience under my belt. Anybody can go online and become an e-mail marketer. It's not really hard.

They'll do better at if they do it well. And you know, even if it's low cost, you get what you pay for. You have to invest a certain amount of money in technology and in education to do this well. Just the ability to do it does not mean that it's been with any level of responsibility.

There are a number of people like my colleagues on the panel here who, you know, are perhaps on one of the highest echelons. There are, you know, the sort of scumbag Spammers who we're all aware of. But there's a huge, gigantic gray area of people in the middle who want to use the internet to market their goods and services, but that doesn't mean that they're marketers. Their primary goal is to manufacture these things or package the things --

MR. SALSBURG: So, from worst practices to best practices, where would the different types of opt-in --

MS. LIEB: All right, I'll start with the worst and work up. The worst practices, and I think there was some consensus on this yesterday among the audience, at least, is opt-out. Opt-out is when somebody's address is added to a list without their knowledge or permission, and it's the recipient's job to tell the sender that they don't want it anymore. This is often not the case, because people have been made to feel very afraid of unsubscribing to things.

MR. SALSBURG: So, I guess with opt-out, it could be the recipient's permission. You just don't know for certain.

MS. LIEB: It depends on the privacy policy of the site. The best case scenario is you have some sort

of relationship with the sender, and they sign you up for something, and you get it, and you can opt-out. The worst case scenario, it's pure Spam. You don't know where it came from or why.

A step above that is confirmed opt-out. Your e-mail address is added to a list of recipients, and you receive an e-mail saying you have been added to this list, you can do something about it, and then there is some sort of unsubscribe option in that e-mail.

There's --

MR. SALSBURG: Ted, you had your tent up, but is the risk with any sort of confirmed opt-out that the opt -- the confirmation is going to be viewed as Spam and never read?

MR. GAVIN: That's a pretty serious risk. You know, it has been common internet wisdom, amassed over the last several years of dealing with Spam, that you don't click remove. You don't respond to unsolicited e-mail that solicits any type of response from you, because you are simply feeding the problem, either through confirming that your e-mail address does connect to a live human being, which means it can then be sold for a higher premium, or that you just simply become a more willing target.

So, with opt-out, by and large, the problem

simply doesn't get resolved through having been added without consent to any list. Having been added without consent to a list and then being told you have now -- you have been added to the list is like slapping somebody and then telling them that you just slapped them. You know, the damage has already been done. You are giving a person the opportunity to do something about it that they have been conditioned over years of experience not to do.

MR. SALSBURG: So, what's the next step that's better?

MS. LIEB: Okay, I would also like to point out, adding to what Ted just said, that the value is on both sides of the relationship. You know, the value of what a consumer is getting, whether they have volunteered or not volunteered to receive something they're getting, is one side of it. The other side of the coin is the quality of the lists that the marketer has, the lists that are going to get the most complaints, the lists that are going to be blocked, the lists that people are going to try to rent or to sell to other marketers that are going to be near valueless.

Right in the middle of the equation is pure opt-in, which is pretty straightforward. You go to a website, there's a thing that says sign up for our newsletter or our specials or our deals, you type in your

e-mail address, hit send, and you're subscribed. That's okay.

The lists are more responsive and they produce fewer complaints, but there are no safety mechanisms built in, and there are plenty of people out there who for reasons ranging from the mischievous to the downright malicious will sign, you know, their friends, their enemies, their co-workers, anybody who did anything they didn't like or, you know, their ex, their boss, up for about a billion e-mails.

These people don't necessarily know how this happened or why or how to unsubscribe or how many things that they're signed up to, and this can lead to people being e-mail-bombed. It is, therefore, not too terribly responsible.

MR. SALSBURG: So, what's better than that?

MS. LIEB: Better than that is confirmed opt-in. You opt-in to something, and because you have opted into it, you get an e-mail, and it says, you have opted into this. Here's your user name and your password, if that's the case, and at least you know what's going on. If you were not personally the person who signed up for whatever it is that you've allegedly signed up for --

MR. SALSBURG: Well, does the confirmation tell

you to contact the sender if you believe that you were opted in inappropriately?

MS. LIEB: Yes, and it should -- everything should always have an unsubscribe link, every piece of communication in your chain.

MR. SALSBURG: So, essentially a confirmed opt-in is really an opt-in that has a confirmation that's an opt-out?

MS. LIEB: Exactly, but it also lets you know what you were signed up for, how many, how much, so that if you did not intend to get this, you have a chance of stemming the tide before it hits.

The gold standard is what I term -- and there is some disagreement on this, but I think it's the clearest terminology -- double-confirmed opt-in. I'm proud to say it's what we do. The user takes an action to subscribe, and immediately receives an e-mail that says, you have subscribed to this, but in case you are not the person who subscribed to this, your subscription is not going to be active until you answer this e-mail to confirm that this e-mail address is really the e-mail address that wants this subscription.

It's a more cumbersome process. The response rate to those e-mails is between 40 and 60 percent, which scares a lot of marketers and publishers to death, but it

makes for the least complaints, the happiest subscribers and the most valuable lists for marketers and advertisers, because these people have proven not once, but twice, that this is, indeed, something that they want and are eager to receive.

MR. SALSBURG: Ben Isaacson, what does the Association for Interactive Marketing's Best Practices Guide recommend in terms of the type of opt-in?

MR. ISAACSON: Well, they certainly -- there's many different ways to determine opt-in, but certainly it is having a prior business relationship is number one, and then I don't want to categorize what Rebecca said, because there's a key missing area here about both opt-in and opt-out, and that is the offline relationship that could be created or extended to the online environment from the retail chain or the teleservices representative or fax, and so within that, there's kind of opt-in and opt-out. So, the opt-in being you fill out the card, you send it back one way or another, you verbally give your e-mail address to somebody on the telephone, and the opt-out being that you have a strong prior business relationship via a catalog or some other mechanism offline, and they send you an opt-out e-mail saying we would like to extend this relationship to e-mail, and please unsubscribe if you don't want to extend the

already-established prior business relationship.

MR. SALSBURG: So, the Association for Interactive Marketing would say that the level of confirmation needed or the type of opt-out depends on whether there's a prior existing relationship between the customer and the business?

MR. ISAACSON: It's based on the prior business relationship, and in my own consulting practice, I urge that there are different layers of permission, permission strategies for, you know, financial services will far exceed that for a B2B niche e-mail newsletter. So, every different communication vehicle should have a different permission strategy.

MR. SALSBURG: Jason Catlett, if the confirmation is sent and it just shows up in somebody's inbox as if it's any old piece of commercial e-mail, what good is it?

MR. CATLETT: Well, it looks just like Spam, and this happens not only because of malicious signing up, it also happens because e-mail addresses are mistyped. People mistype e-mail addresses, their own e-mail addresses, into forms all the time, and john64@aol.com causes some Spam for john46@aol.com, and when john46 gets it, this so-called confirmed opt-in looks like Spam to them, and it's functionally like Spam.

If you don't opt-out, then you are going to get more. So, we're back into the DMA's happy hunting ground of Spam them until they scream.

MR. SALSBURG: Does anybody on the panel know whether there have been studies done to show what percentage of people that get the confirmations actually read them?

MS. ZORNOSA: Yeah, this is an area that we actually have a lot of experience with. We organize our entire customer base against IP blocks where if you are a double opt-in customer, you go to a very specific IP block. If you're someone whose membership is not double opt-in, you mail out of another one. And in fact, if you're -- if you have a list and parts of it are double opt-in, you will go out of one block and the other part will go out of the other block, which gives us a very, very good case -- you know, aquarium in which to see what the response rates are if you're opt-in and if you're not double opt-in, and we've encouraged our customers a lot to double opt-in wherever they can, because it's very clear that the response rates are 25 to 33 percent higher on the double opt-in block for the names that are on the double opt-in block, even when our list is divided between the two.

Now, we've also had a chance to sort of

experiment with you have a list that is -- that has been gathered in an opt-in basis, and you want to confirm it -- you want to turn it to double opt-in, and how many of your customers are you likely to lose in that event? And it's very interesting that I would agree with Rebecca's statistics that you will lose, you know, 40 to 60 percent of your list in the process.

Now, in our case, you're not losing them, because you're able to continue to mail them, but you are not mailing them out of the block that has the benefit of being the double opt-in block.

Now, one of the things that we've learned is that when you have a very good list that has a great relationship with its customers, you will get, you know, 60 percent of them to convert to double opt-in upon a request, but what's equally interesting to us is that the, you know, 40 to 60 percent who do not convert are not necessarily saying that they don't want your e-mailing. You know, there are very specific reasons why those people don't convert, which is why we have continued to offer the hybrid option.

So, for instance, e-mail may be grandmother-proof, but a confirmation opt-in that requires her to open something that looks a little form, that then has instructions for her, that has a link

inside, for some demographics, they are less likely to follow all the steps.

The other thing that is sort of, you know, particularly perhaps troublesome is that, you know, an e-mail service provider, you know, such as mine -- in fact, most e-mail service providers such as mine are on one blacklist or the other, and so the problem that the invitations never get to the person that you are now inviting to participate in the gold standard that, you know, of permission is also another problem.

And then, of course, you have just got the fact that some people are on vacation or some people don't rate that particular e-mail or that particular invitation will go into a bulk folder as part of the -- part of the phenomenon as well.

MR. SALSBURG: We've received an e-mail that we all scream into the microphone, because apparently out in the ether world, it's difficult to hear.

Ted Gavin?

MR. GAVIN: Anna raises an interesting question, and I'd like to ask this directly to her. Given that your business can be materially harmed by the poor list practices of your customers, how do you -- how do you deal with that just as a business? I mean, you know, the concept of the mail service house is a fairly

new one, and, you know, SpamCon Foundation, our constituents are recipients, legal professionals, marketers and network operators, and mail service bureaus or mail service providers are in this nebulous space between that and also spanning all across it.

So, I'm curious as to how you reconcile your business model with the fact that what you're sending is not your own, you actually have no control over it, and you do face very real material harm? As you mentioned, you're on more than a few blacklist, and your firm is a frequent topic of conversation among those communities.

MS. ZORNOSA: I think it's a very, very good question. I mean, to be big in sending e-mail is to be the subject of a lot of criticism and a lot of debate about your practices, and it's something that -- oh, thank you -- I said that to be big in e-mail is to be subject to a lot of criticism and a lot of debate about your practices, as I would note, I think it very well should be.

You know, companies like mine -- like the ISPs, we sit in the very middle of a spectrum that starts with a sender, you know, and ends with a recipient, and we do an awful lot of education and an awful lot of policing of our own customer base to try to make sure that their practices are, you know, acceptable enough to

stay on our service and acceptable enough to their end users.

You know, one of the things, of course, is we try as much as possible to encourage the use of double opt-in, because we believe at the end of the day, the responsibility for whether or not the mail is delivered is -- should be that of the sender. Their practices should determine whether or not that mail gets delivered.

Today, you know, if we put a good sender next to a bad sender, it's very likely that the good sender will be impacted by the bad sender's practices. So, that's why we've told our customers that more and more, if you will double opt-in, we will send you out of a block that is 100 percent double opt-in. We will warrant to the ISPs and to the community that that block is double opt-in, and what we're trying to do is create a set of aggressive carrots and tell our customers, if you don't want to be blocked, then your real recourse at the end of the day is to confirm opt-in the name.

Now, what we would love is to have industry participation in that, because the more that we can say to our customers you confirm opt-in, and the result is you're going to get deliverability, then the more that we will all together be truly solving this in a way that matters an awful lot to my customers and that through the

practices we put in place, I can ascertain will definitely be tempting to them and conducive for them to follow it.

MR. SALSBURG: The big carrot that you offer is the ability for your clients to get past blacklists, and --

MS. ZORNOSA: I would say that's one, but let me let you finish.

MR. SALSBURG: Okay, well, as one of the incentives, a lot of consumers will have opted in and forgotten about it. Is it a best practice to send periodic reminders to the consumers saying, you know, you opted in, do you still want to get this e-mail? And if you don't get a response, stopping the e-mail?

MS. ZORNOSA: You know, it is not a best practice today, and it is not a practice today. Most people who double opt-in, you know, view that the relationship has started on a very, very firm permission basis and that you perhaps continually, you know, sort of ask is a form of Spam in and of itself.

Now, we can debate as a name gets older, you know, when a name is two years old, should there be some sort of trigger for re-accepting them? I think we're going to get there. You know, the majority of lists on our system today are not older lists. Older lists are

very different than young lists in terms of their behavior and those kinds of things, and I think -- and I think there's room for discussion of that as a best practice.

MR. SALSBURG: What if your response rates indicated that a certain e-mail account hadn't opened a message from you in, you know, six months?

MS. ZORNOSA: You know, that is a -- that is a question that our senders would ask themselves, and I can answer that question for you in the case of me being the hypothetical user of my service and having a list. You know, I believe if I was a user of my service and paying a high CPM and I noticed that my list was not being opened anymore, I would take definite steps, you know, one of them perhaps to ask for re-opt-in, but of course, if they're not responding, then that's not going to solve the problem.

MR. SALSBURG: So, because they're paying a higher message cost for having it sent, your client has the incentive to purge the list of nonresponsive --

MS. ZORNOSA: My clients are making economic decisions every day based on the responsiveness of their lists.

MR. SALSBURG: Michael Mayor?

MR. MAYOR: I had forgotten I had put my name

bar up there. I will say this. I will say that, you know, I'm in the business of managing for quality. I need to have responsive lists to rent to the end mailer, and double opt-in makes good sense not just for a privacy standpoint. It makes good sense from a business standpoint. They're not going to get added on my list if they have filters, because they're not going to get the confirmation. They're not going to get added to my list if we're being blocked or if it bounces or if they have a typo in the address. It makes good business sense to have double opt-in, and that adds to the responsiveness of the list, and you know, I think that's what we're all talking about.

We're not talking about building the biggest list and how to get people on my list. I want -- I'd rather have 100,000 great responders than 10 billion so-so responders, and I think that's really what it's all about. It's about having the best list and what do you do to put that together. You know, I'll tell you this, about a year ago, we realized that the delete issue was a big problem, that people would not delete because they were afraid that that was an indicator and that they would be added to a Spam list.

We took it upon ourself to remove millions of names from our database, because they were nonresponsive

for our mailers. That's the name of the game. I will not be in business if my lists do not respond, and that's really what it's all about.

MR. SALSBURG: Ben Isaacson, where should the breadth of an opt-in be disclosed? How should a consumer be informed that their e-mail address will be used when they opt-in under any of the various types of opt-ins?

MR. ISAACSON: Well, I mean, certainly you do that during the confirmation process, as we have talked about, but during the course of a communication relationship, there are many different ways in which the sender can identify themselves. I think for the known brand e-mailers, there's no question that they did opt-in and that that information can be at the bottom of the e-mail message, and they can know this is where you can opt-out and this is the e-mail address that you are subscribed as.

MR. SALSBURG: But in the initial opt-in, would it be good enough to stick in the privacy policy, the uses that would be made of the e-mail address, or should that be disclosed right alongside of the fields where a consumer would enter the e-mail address?

MR. ISAACSON: Right, during -- there was section solutions set for responsible e-mailers, and one of them is at the point of collection, there should be

notice of how that e-mail address is going to be used, and during that -- during the discussions, we -- at the time, this was almost three years actually, we decided that having a link to a privacy policy and having the information in the privacy policy would be acceptable.

MR. SALSBURG: It would be acceptable?

MR. ISAACSON: Yeah.

MR. SALSBURG: Ted Gavin, what's your view on that? Should the uses of an e-mail address be disclosed in the privacy policy or somewhere -- somewhere else?

MR. GAVIN: Well, they certainly do need to be disclose understand a privacy policy, and I think the FTC has done a pretty thorough job in those cases where it was warranted going after those firms that required corrective action for not adhering to their own privacy policy, especially with respect to their use of e-mail addresses.

However, there needs to to be more. Privacy policies can be very difficult to read. A lot of people never read them. And while consumers should absolutely read privacy policies whenever they're giving any type of personal information, we all know that not everybody does. No one reads every page of a contract unless they've got a lot of time to spare.

When running an e-mail list, especially

newsletters or lists of a commercial nature that you are either renting or selling, which -- and selling lists is a really bad thing to do, renting is marginally better, but not really as good as creating your own list for your own purposes, it's important that if you're not using those recipients' addresses frequently, you do remind them. If you're going to -- you know, if you're running a newsletter and there's a long gap, you should certainly have in each newsletter, you're receiving this because you subscribed, and here's how you stop subscribing if you want to.

If you're doing legitimate e-mail marketing, having some sort of reminder to the members of your list is pretty important, because you certainly don't want the stigma of being labeled Spam because somebody forgot or they haven't gotten an e-mail from you in six months because you haven't had a customer who required that list in six or eight months.

So, you know, there's -- and I think that the earlier statement that Michael made about removing dormant addresses from their lists is certainly a best practice for marketers. You know, if you've bothered to capture an address and you know that you're only going to be effective if you don't alienate your potential customers, then doing that type of list housekeeping is

not only a best practice, but is a means to survival.

MR. SALSBURG: Anna Zornosa, is disclosing the frequency that messages will be coming a best practice as well?

MS. ZORNOSA: Yes, in fact, what we recommend is that every customer should be greeted with some sort of memorable, you know, hello, even if they have already confirmed opt-in, regardless of the method that they've come onto your list, they should get a message from you that says what frequency they can more or less expect, that reminds them of the content, that reminds them what to do if it ever should be subscribed, that restates the privacy policy that you have on that name, but yes, I think that having the customers understand something about the frequency very early on in the process is very important.

MR. SALSBURG: Do either you or Michael Mayor purchase lists or these lists?

MR. MAYOR: Absolutely not. I -- we don't practice the frequency. I think that we give the consumer, the list member, choice. They have an opportunity to opt-out with every message we send. And so if we're doing a bad job, if we are basically pummeling these people, we're going to have attrition, and, you know, after all the opt-in and confirmed or

double opt-in, you know, you -- there's something outlandish that you have to do. It's called managing your list, and you've got to -- you know, you've got to basically look at all the moving parts, and you've got to act on them.

So, we gave them pure choice. They can get off one list or every list in our database with every mailing.

MR. SALSBURG: Let's move on to unsubscribing. Michael Mayor, what options do you offer consumers to unsubscribe from lists when they receive them?

MR. MAYOR: We give them two. We -- there's a link that they can click in the e-mail, and they can send the e-mail to an e-mail address.

MR. SALSBURG: Okay.

MS. ZORNOSA: And as a service provider, we insist that everyone who uses our system embed a one-click unsubscribe that's individual to the recipient of that e-mail in their newsletter. What we have found is multiple ways of unsubscription are, you know, desirable.

So, there is a click within the newsletter. There is a reply to, unsubscribe, service end function. We have across Topica services the ability for you to unsubscribe from all of a certain type of products. You

may want to unsubscribe from newsletters that our customers publish but not unsubscribe from the discussion groups.

So, we give them the option of doing either. We also give them the option of just getting off of everything that is in the -- that is in our database that you've ever subscribed to.

MR. SALSBURG: Is there an economic reason why unsubscribing should be made at least as easy as reporting a message of Spam?

MS. ZORNOSA: Absolutely.

MR. GAVIN: I think that predicates that reporting a message as Spam is easy.

MS. ZORNOSA: That's -- yes, I think that's why I was a little confused.

MR. SALSBURG: Assuming there are some ISPs out there where you can just click, this is Spam, on the message, should an e-mail come from with an equally prominent button saying unsubscribe?

MR. MAYOR: Maybe we could have a contest for unsubscribes, too.

MS. ZORNOSA: We live in very confusing times, you know? Unsubscription in -- from any newsletter that's published on our service is a one-click process, and it is something that, you know, that is the -- it is

the most important thing for us always to keep functioning and keep functioning absolutely correctly.

However, you know, the subscribers are starting to hear more and more that unsubscribing will propagate e-mail they don't want, and it's become not a very nuanced statement, and I'll tell you what, you know, from the work I know that the FTC has done, looking at that very fact in your Spam sting, whether or not someone unsubscribing actually propagated their -- you know, had more of a propensity to achieve Spam, I'm told that that's not the case, that scientifically, you saw that that was not the case.

However, you know, it is becoming more of a belief in subscribers' minds that they can't do that. Not everyone practices the same practices that we do. We wish, you know, that were not the case. From our perspective, life would be much easier if, you know, AOL, for instance, was being told, this is Spam only when this is Spam and being unsubscribed when they really wanted to unsubscribe.

However, it's a reality of the field, of the marketplace that we live in, that that's probably had to be, you know, had to be said.

MR. SALSBURG: Assume that you as an e-mailer are sending out e-mail to a single consumer from various

lists on behalf of various consumers. Does unsubscribe apply to one list, one -- one client on your behalf?

MS. ZORNOSA: Yes.

MR. SALSBURG: Or everything?

MS. ZORNOSA: An unsubscribe to a particular communication newsletter, discussion group, applies to that particular newsletter/discussion group, unless you come to the Topica site and do a product unsubscribe or a global unsubscribe.

MR. SALSBURG: So, that would be one of the options if you went to the links?

MS. ZORNOSA: That's right.

MR. MAYOR: We do both. We give them the opportunity to get off that one list that generated that e-mail, or they could click a link and look at everything that we have on them in our database, and they can just, you know, remove themselves from everything if they like.

MR. SALSBURG: Ben Isaacson?

MR. ISAACSON: I just want to add on top of what Anna was saying about giving the users an option, I think that's the -- the trend is to not only give them an option but to even offer them preference management, and I mean the truth is, everyone in this room has more than one e-mail address, and often want to change where certain newsletters and certain commercial solicitations

are going. So, changing your e-mail address, even if you're going on a long vacation and you want to, you know, stop that from being sent, there are many different preferences that you can set.

And, of course, with the network providers that have multiple lists, you might be on ten different types of lists. So, sending them to a preference page where they can then remove themselves from those particular lists they no longer have interest in is something where the marketplace is going.

MR. SALSBURG: Rebecca Lieb?

MS. LIEB: If I can add to that, we certainly have all of those options, click here to unsubscribe, and you're unsubscribed instantaneously. We have a manage your subscriptions button where, you know, as my colleague said, you can view and manage and change anything.

However, we're noticing people have been so conditioned not to click the unsubscribe buttons that they would rather e-mail us and say, please unsubscribe me, without specifying what they're subscribed to or what e-mail address should be unsubscribed. It's really exciting when they actually e-mail you from the address that they are subscribed to, which then turns into a time-consuming, costly and cumbersome process.

We have a desk of people that help our subscribers do whatever it is they're having problems with. Those people then have to go into the records, find out who this person really is, what they really want, what e-mail address is involved, and often you can't unsubscribe them if all you have is an e-mail address which is an e-mail address that is an unsubscribe to anything at your company.

So, people I think are complaining that they're not getting unsubscribed when they're actually with these nine-year-old requests making it difficult if not impossible for a publisher to do that without three or four more e-mails back and forth, which can then anger a customer, because they don't want to hear from you again.

MR. SALSBURG: Let's move on to e-mail appending, because we're -- our time is fleeting. Ben Isaacson, what is e-mail appending?

MR. ISAACSON: Well, there's a formal definition on a website at Interactivemarketing.org. It says, "E-mail address appending is the process of adding an individual's e-mail address to a marketer's existing database. This is accomplished by matching the marketer's database against a third-party permission-based database to produce a corresponding e-mail address."

In other words, if you have an offline relationship and you want to extend that to the e-mail environment, you can then work with a third party that has opt-in permission-based lists and try and find those missing e-mail addresses, have that append provider send a message on behalf of the brand marketer and then ask them to either opt-out or opt-in. After a certain period of time, those e-mail addresses are either transferred or I guess in Mike's case they are not transferred but can be used by the marketer.

MR. SALSBURG: Let's say that I purchase a toaster oven, and I fill out the warranty card, and the warranty card includes all fields you usually see, home address, business phone, e-mail, and I leave the e-mail address blank. Haven't I indicated I don't want to be contacted by e-mail, leave me alone, contact me by, you know, less intrusive means, like by telephone to my house?

MR. ISAACSON: I mean, to me, just personally, it often means that you don't have an e-mail address, but -- because there are 43 percent of people who aren't hooked up to the internet, as we learned from Pugh, so that's the first impression that you get.

MR. SALSBURG: Ted Gavin?

MR. GAVIN: I saw a short article in one of the

business publications a week or so ago that talked about how permission-based e-appending, where I have given you my paper address, I have given you my e-mail address, actually produces substantially higher conversion rates.

And if it is entirely permission-based, I suppose it's okay. In fact, it's a very valuable and legitimate marketing tool. Anything but that really has significant, substantial and almost uncontrollable privacy concerns on the part of the consumer. I have four e-mail addresses. How can you possibly know which one of those is appropriate to send things to me that we may or may not have already established a prior business relationship on?

You know, prior business relationships exist in a myriad of companies, different products, different sectors. If you get my e-mail address and you decide to send me a catalog to my paper address, my physical address, based on my e-mail practices, that could be fine, that could be horrifically embarrassing, that could damage various aspects of my personal or professional life -- hypothetically speaking, I don't have that problem personally -- and it seems to me that this has gotten to the point where we are saying simply because we can do this means we should.

You know, on behalf of the various constituents

that I'm here representing, I suspect that we need to take the position that we are not the arbiters of the technology that is at our disposal. We are the servants of the people who will use it. And this does need to be somewhat protected and more moderately applied.

MR. SALSBURG: Jason Catlett, let's say I fill out this warranty card, and I give my e-mail address, but when you as the e-mail marketer attempt to e-mail me, it bounces. Isn't it appropriate for you then to try to find a correct e-mail address for me?

MR. CATLETT: Well, first, I'm not an e-mail marketer, but supposing that I were, warranty cards -- I mean, they're just a privacy quagmire, because they generally do not disclose the purpose for which the information is to be put, and there seems to be some other reason --

MR. SALSBURG: Well, let's say instead of a warranty card, then, I try to -- I apply to enter a contest in a box and win a trip to the Bahamas, a highly legitimate contest.

MR. CATLETT: Yeah, well, I mean some of the websites that offer sweep stakes get you to push a button saying yes, I enter, and if you read the privacy policy, it basically says we'll do whatever we want with any information we get from you or about you via any means

whatsoever, and you absolve us of any liability, blah-blah-blah-blah. So, basically it's a rape and pillage clause that you're consenting to buried in the fine print, which is unfair.

Also, I'd like to come back to this whole idea of e-mail append. It's a really bad idea. If you subscribe to a magazine, for example, you give them your physical address and name, and then they start sending you e-mail that they got from someone else saying wouldn't you like to get our e-mail updates, that's just wrong. If you wanted to get that, you would have gone to their website. So, e-mail append is a privacy invasive practice.

It also has other privacy problems, which is if you get the wrong address, then -- and these data -- these lists are not 100 percent correct, then they may -- the company may establish a relationship with the wrong person, and I'd refer you to a story in the Wall Street Journal a few months ago where Citibank used e-mail append to send out some e-mails, and they weren't all correct, and that went into -- that went into some litigation I'm told.

MR. SALSBURG: Rebecca, does that mean when you e-mail append, essentially you're sending an opt-out?

MS. LIEB: One would hope that you could opt-

out. There are some examples I think that are congruent with your warranty card. I was at a conference last week in which somebody at AOL complained that a major retailer, a very major global retailer, was sending e-mails through AOL, 60 percent of which were sent to nonexistent AOL addresses, and that's because this retailer had had an in-store promotion in which they had something like 10 percent off your purchases today if you give us your e-mail address.

You know, there are rapacious marketers, but consumers are not always as stupid as people give them credit for. For 10 percent off, I think somebody can be induced to write anyone@anywhere.com and hand the card to the lady, but that doesn't help marketers build lists. It does not help marketers keep clean lists, and with e-mail confirmation, list hygiene is taken care of right out of the gate. It certainly doesn't help ISPs like marketers any more when they're dealing with an old -- more load on their already overburdened servers. So, why append, you know, under certain circumstances can possibly work with a great deal of permission and transparency, it has to be handled even more delicately than straight web-based transactions.

MR. SALSBURG: Michael Mayor, e-mail appending, a good thing or a bad thing?

MR. MAYOR: Bad. You know, this is where I part company with most of my colleagues and everybody in the industry. I think e-mail appending is based on one principle, that permission is transferable, and it's not. It is not, absolutely not. I think that if I gave my friend Tony over here the car keys and said go pick up something for me, he has no right to give me car to somebody else, and that's what this is about.

E-mail appending is a black and white issue to me. You either have permission or you don't. The only people that are not getting e-mail appending are the direct marketers who do it offline, and everybody else -- everybody else in the world gets it. It's the wrong thing to do, and it's not effective.

MR. SALSBURG: Okay, we are about out of time, so why don't we turn it to the audience -- oh, five more minutes? Jason, why don't you make a parting shot, and then we will turn it over and hear some questions.

MR. CATLETT: Yeah, Michael is correct, it comes from the paper world of direct marketing where an append is the ability to buy the number of children in the household or the number of cars or the income of a particular place, but e-mail, it shouldn't be done.

The existing business relationship exception that seems to be claimed is just not appropriate, and I

hope that any new legislation, that there's no exemption saying that you can send unsolicited e-mail to someone with whom you have an existing business relationship of any quality offline.

MR. SALSBURG: Okay, let's turn it over to some questions. Mona, back there?

MS. ARBON: Rebecca had made the point --

MR. SALSBURG: Can you identify yourself?

MS. ARBON: I'm sorry, I'm Margie Arbon with MAPS. Rebecca had made the point and she made a differentiation between opt-out and what she called confirmed opt-in, which the only difference is a sign-up on a website. To the user that did not sign up that either maliciously, accidentally, whatever, got forged subscribed to, say, 900 mailing lists, what's the difference between opt-out and what you called confirmed opt-in?

MS. LIEB: When you don't receive a confirmation, you have no way of knowing what's coming from where how frequently. At least a confirmation, if somebody volunteered your information, would give the victim some recourse prior to receiving, you know, an overwhelming load of subscriptions that they didn't solicit.

MR. SALSBURG: This gentleman right here?

MR. KELLY: Hi, Bennett Kelly, I'm an attorney in Los Angeles. One question, in talking about the different levels of permission from near the bottom to the gold standard, as Congress considers regulating Spam, what do you think would be the appropriate level for Congress to require?

MR. SALSBURG: Who wants to take a quick ten-second stab at answering what Congress should do?

MR. GAVIN: I can pitch something in. You know, we're a nonprofit organization, so we don't lobby, so this is all really just theoretical conversation for me now; however, we -- SpamCon Foundation are signatories to the open letter that was issued on Tuesday to Congress and to the public with the Coalition Against Unsolicited Commercial E-mail and JunkBusters saying that any legislation that isn't going to legitimize and legalize opt-out does need to be opt-in. I certainly think confirmed opt-in would be the utopian ideal there, and it would be the most respectful of the cost structure of e-mail marketing.

MR. ISAACSON: And speaking on behalf of myself, as I am no longer a registered AMDA lobbyist, I believe that having a prior business relationship is sufficient, as long as the recipient knows who you are and can trace back and the sender can trace back where

that relationship started, then we are starting from a good point, and then in the future, we can look to more stringent matters, but to get something done today, we do want something passed -- I want something passed in this Congressional session, and in order to do that, we have got to start somewhere, and I think that's prior business relationship.

MR. SALSBURG: Okay, we have a question that came in over the internet to us. One of the ways that UCE is dealt with by bouncing it. At what point should a bounce be considered a message to the mailer that they should stop mailing to the recipient?

Anna Zornosa, if you get a bounce, do you just take that person off the list?

MS. ZORNOSA: You know, a bounce -- of course, there's different categories of bounces, and there are -- there is enough divergence going on that -- in terms of the bounce strings that you get back from the ISPs that it is not always clear, you know, that what is getting bounced back to you is being bounced back to you because the mailbox is permanently disabled or temporarily.

So, where it is clear that the mailbox is permanently disabled, we immediately disable it. Where it is not clear if it's a temporary or a permanent

relationship, we have a set number of times that it can bounce and then it is taken off, and it is disabled.

MR. SALSBURG: Michael Mayor, is that typical?

MR. MAYOR: That's typical. I mean, there's hard and there's soft bounces. A hard bounce is indicative of the e-mail address not being there or invalid. A soft bounce is that it's there, the mailbox might be full. Most marketers will delete or remove on a hard bounce, and they'll have a set number of bounces for the soft bounce.

MR. SALSBURG: Okay, let's take another question. Front and center, please wait for the microphone, and identify yourself, please.

MR. HUDSO: Hi, Carl Hudso with America Online. I work in the e-mail operations department, and my question really centers around the thing that I find interesting on these panels, when people disagree, it's sort of boring, because it's sort of easy, but the one thing everybody sort of agreed to, which surprised me, was on the labeling aspect, and I wonder, I understand some of the problems with trying to label commercial e-mail with advertisements versus a newsletter with an ad and so forth.

What about an effort to try and label something that is a bulk e-mail as opposed to a personal one?

AOL's actually tried to do that ourselves in an effort to try and allow our members to be able to sort mail just like you might when you come home and read snail mail that comes in your mailbox. So, what do you folks think of that?

MR. MAYOR: What value is it to the recipient to know that you sent 10 million or one? You know, I mean, this bulk term is another term -- there's two terms that need to be X'd out of the dictionary right away. It's bulk and it's opt-in. Opt-in has no meaning anymore. But bulk, you know, define bulk. Is it ten or is it 10,000? You know, I think that when you're sending e-mail that you have permission to, what is the problem?

If we get into subject line labeling, Spammers are smart people. They -- you know, they've forged headers. They can forge a subject line.

MR. ISAACSON: I think for AOL, you read the headers, the actual header codes, and so if we were to talk -- all talk about certification, I know there's many programs being offered, where you and the other ISPs would all agree on reading a label of a bulk sender as a certified type sender, then that might be a different type of labeling that would be transparent to the customer.

MR. SALSBURG: Okay, let's take another

question. There's a gentleman over here. The microphone is on its way.

MR. IVERSON: I know we had talked -- excuse me, I'm Al Iverson from Digital River. I actually do a lot of e-mail marketing for our clients, and I know there's a lot of talk about the this is Spam button on stuff like AOL, and I'm wondering if any of the other e-mail marketers feel that it might be appropriate to have some sort of trusted unsubscribe program or similar to that. You know, is there something where us as mailers opt-in to it, where we know that we get this, we are going to deal with it, it's an unsubscribe, it won't get bungled? What are your thoughts on that?

MR. SALSBURG: Rebecca, do you want to describe what a trusted unsubscribe program is briefly?

MS. LIEB: I don't think that there is a firm definition of a trusted unsubscribe program, but I think that one should be concocted, and I am going to give Ben credit with this, who wrote an article for one of my publications recently describing the various unsubscribe mechanisms that exist and are out there and essentially saying that the industry does need an unsubscribe standard. Again, I don't think this was on anybody's radar screen two years ago.

MR. ISAACSON: And even prior to an unsubscribe

standard, because I know that's difficult and there's liability issues, if next to this Spam button there could be an add to approved senders button very visibly posted, that would be, you know, that would be good, too, to help expediate the white list process.

MR. SALSBURG: Well, that brings us to the close of the session. Thank you very much for all coming in.

(Whereupon, there was a brief pause in the proceedings.)

MS. HONE: Thank you, everyone. My name is Lisa Hone and I'm an attorney with the Division of Marketing Practices here at the Federal Trade Commission. Thank you all who've hung in through the day. This is our last panel of today and tomorrow will be the third and final day of the FTC Spam Forum.

This panel is a little different in a couple of ways from all that has come before and all that will come after. This panel is focused specifically on wireless Spam and, obviously, there are overlapping issues when we think about wireless Spam, but there are also some issues that are distinct to wireless Spam. So, this panel, and it's a large panel, has a large task in front of it in the next hour and a half or so.

What we're going to do is talk about wireless

Spam from soup to nuts. And unlike most of the other panels, there's not going to be so much give and take between the moderator and the panelists. Our first four speakers have volunteered to give us some real introductory information about wireless messaging and wireless Spam and our next five speakers will comment on what's come before and issues that are of particular interest to their organizations or portions of the industry.

I'm going to do a quick introduction of everyone just so that you know the line-up and then I will ask our panelists to take it away. Our goal is to make sure that we leave plenty of time for questions. So, wish us luck.

First up will be Mike Altschul, who's a Senior Vice President for Policy and Administration and the General Counsel of CTIA. I will remind all the panelists that you have to speak really close to your mic, and I'm obviously having a little trouble doing that.

Second will be Jim Manis, who is the Chair of the Mobile Marketing Association and with M-Cube.

Third will be Jiro Murayama, who's a Manager at NTT DoCoMo, who's going to talk to us about the Japanese experience. We have a lot to learn from the Japanese experience with wireless Spam.

Fourth will be Rodney Joffe. He's on this panel as a consumer who's dealt with wireless Spam. Rodney is the plaintiff in a lawsuit in Arizona alleging that a company, Acacia Mortgaging, wireless Spammed him repeatedly. I will let Rodney get into the details there. But he is also a computer scientist and has been a member of the direct marketing industry. So, he comes at it with a very global view.

Then Margaret Egler, who is with our sister agency, the Federal Communications Commission. Margaret is the Deputy Bureau Chief for Policy in the Consumer and Governmental Affairs Bureau. I have to read that because Margaret has a history at the Federal Communications Commission. She's had a number of different jobs. But in all of her jobs, she's worked closely with the Federal Trade Commission on consumer protection matters. So, the title is important but what's most important to us at the FTC is her consistent cooperation with us on consumer protection matters and, obviously, the FCC has an interest in wireless Spam and consumer protection issues, as well as industry issues.

To my left is Andrew Blander, Corporate Counsel for AT&T Wireless. Then Marc Theermann, who's with YellowPepper. Carl Gunell with Telemedia and Carl has been very helpful to us over the course of the last

several years in terms of providing information and suggestions to the Federal Trade Commission staff about all sorts of mobile marketing issues. And, finally, at the end, batting clean-up is Al Gidari, who's a partner at Perkins Coie in Seattle.

So, Mike, if I could ask you to take it away.

MR. ALTSCHUL: Thank you, Lisa. And on behalf of CTIA, I want to thank the commission for inviting us to participate. We started life in 1984 as a typical trade association representing what were there called cellular carriers. Three years ago, CTIA recognized that wireless text messaging and internet access was poised to become a major source of growth for wireless carriers and consumers. Text messaging, in particular, was taking off around the world, and in the U.S., wireless carriers were introducing these services as they upgraded their networks. Moreover, the new, next generation wireless technology promised to make internet browsing a faster and more user-friendly experience for wireless customers and to convert more customers to these new services.

CTIA was so impressed with the promise to wireless data that we changed the name of our association to reflect the importance of the internet. Didn't change the initials, didn't buy any vowels, we just added -- we changed the I from Industry to Internet. So, we now for

the Cellular Telecommunications and Internet Association, and this reflects the importance of the internet and wireless data to the wireless industry today.

While the average wireless customer continues to shift more and more voice minutes to wireless networks from wire line networks. It's the growth in wireless data that has been the most explosive area for the wireless industry. Today, all six of the national wireless carriers support internet access and two-way text messaging services and they're actively promoting wireless data capabilities to customers.

I walked out of my office today at lunch, went by a T-Mobile retail store and I was caught, knowing I was going to be with you this afternoon, in the window with a banner that said, limited time offer, unlimited internet access, text messaging, $10 a month. So, I went in -- and this is true of, I think, all of the national carriers, but they have a big promotion, not advertising just for T-Mobile, they have a much more attractive spokesperson than me, but to give an example of how popular these services are, it is the service du jour, at least in the T-Mobile window, for the month of May.

While we have different interfaces, different technologies in the United States, it's fair to say that the wireless industry is supporting internet access at

data rates of about somewhere between 40,000 and 60,000 bits per second. It's fair to say wireless carriers are still experimenting as to how they charge and how customers want to pay for this service.

I'm an antitrust lawyer by background, so we usually don't ask our members how much they're charging. We certainly never ask them that in front of their competitors. So, I've done a little research by going to kiosks and the internet and because it's a dynamic industry, I think that these rates change, you know, almost weekly. But some carriers, such as AT&T wireless, they charge $2.99 a month, plus two cents per thousand bytes to $19.99 a month, $20 for eight million bytes transmitted.

Other carriers, T-Mobile and Sprint, for example, charge $10 a month for unlimited data use in addition to their regular calling plan fees. Verizon Wireless provides data service as an extension of voice service, sort of as a minute, whether it's being used for data or voice.

We think there are a number of reasons why consumers are using their wireless phones and devices more and more to access information on the internet and send two-way text messages. First, of course, it's the consequence of faster wireless networks. Second,

improved customer interfaces. The way the devices present and organize data, the introduction of color screens, larger devices that are similar to PDAs and have better resolution and innovative input solutions, coupled with the greater processing and memory of the devices themselves.

In addition, we have air interface cards that now permit laptops to access the internet over wireless networks and give users a feel that is similar to a wired internet connection.

The first data service that wireless users typically experience is what we call SMS text messaging. SMS is an acronym that stands for short message service. To provide an idea of how explosive this growth has been, in December 2000, roughly just a little more than two years ago, CTIA took a survey of our members to see how many text messages were sent in the month of December. We counted 14.4 million messages. One year later in December 2001, the traffic had jumped from 14 million SMS messages to over 252 million messages. And this past year, in December of 2002, the traffic grew four-fold from the year before to more than a billion messages in the month of December 2002.

And we see this growth continuing the -- if you plot it -- I don't have a PowerPoint presentation

today -- but it's the proverbial hockey stick, with the growth in messaging being fairly flat and slow on the uptake and now going straight up.

Having said that, in the U.S., we still have a long way to go to equal the 27 billion SMS messages that are now being sent every month in the European community. We know where this growth is going to come from. We estimate that about 20 percent of U.S. wireless customers are using SMS text services and sending these messages today.

Included in this group of one out of five users are young adults in the 18 to 24-year-old demographic. In this group, 45 percent use text messaging and they use it far more extensively than any other demographic group. We anticipate that as more and more users come on into our services that we'll see the same kind of uptake in usage.

Last year -- and this also is a reason that we've seen the messages take off in the U.S. -- we were able to work with our member companies to facilitate inter-carrier SMS messaging. Prior to this effort, it was hit or miss as to whether or not a user could send a text message to a customer on a different carrier's network. But for the past year, all the national wireless carriers have supported inter-carrier SMS

messaging. So, customers don't have to wonder or worry about whether or not the recipient of the text message is on the same carrier's network as they are.

To date, the wireless industry and its customers have not had that many problems. We're not saying that we're perfect or have had no problems. But we have not had the kind of problems with unsolicited wireless messages that certainly has been the average internet user's experience. This isn't because of good luck, but rather because wireless carriers are constantly taking steps to prevent the explosion of Spam that has invaded the wired internet. And wireless carriers have done this because they recognize their strong incentive to protect their customers from unwanted messages.

As I mentioned a minute ago, we still have most of the market; most of the current users of wireless services are voice customers. We want to convert them to the benefits of using their devices for both voice and data. To do that, the industry has to convince customers to upgrade their handsets and devices to devices that support data services, SMS and internet browsing, and then to use these services. If Spam ruins the user experience, the opportunity for wireless data will be lost. Customers simply will not use their devices for data services.

We have the benefit in the U.S., in a perverse sort of way, of being a bit slower to roll out and introduce these data services than mobile phone carriers in Europe and Asia, and we'll hear in a minute about DoCoMo's very successful roll-out and then their experience with Spam in Japan. And having been a bit later to roll out these services, we've had the benefit of the experience of other carriers in other markets in learning how to deal with unsolicited messages.

As I mentioned, we, at CTIA, facilitated inter-carrier SMS messages. In the U.S., these messages are defined as peer-to-peer messages with 160 characters. That's the least common denominator message set or message link that the various technologies will all support. Because carriers typically charge a per message fee for mobile-originated messages, the economics of using a mobile network to send Spam messages is entirely different from the internet model.

Moreover, while it's possible to send an SMS message to a wireless user from the internet, wireless carriers require messages to go through a carrier owned and controlled gateway to reach their customers. This gateway has been designed to be user-friendly for sending individual SMS messages addressed to a wireless customer and using the customer's phone number as the address.

But the gateways do not support multiple messages and have been designed to detect and filter multiple identical messages. So, from the initial gateway to the public internet, carriers are able to identify and filter identical Spam messages.

So, it is possible to send Spam to wireless users, but if the systems work as they're intended, only one or two messages at a time will go through and the process is so cumbersome that it does not become a problem for users. In this regard, the architecture of a wireless network allows wireless carriers a level of control that is not available on the public internet, which is really designed to be open and free of these gateways. And we've checked and all of the national wireless carriers use intelligent software that filters the Spam at their gateways.

As an aside to the telecom lawyers in the audience, I should suggest that wireless carriers can filter messages because they fall into the category of an information service. It's a message that is stored and then delivered to users and this fits the information of an information service. In contrast to information services, the Communications Act defines regular phone calls as telecommunications services, and when common carriers provide telecommunications services, they do not

have the right to filter content.

Congress addressed carriers' ability or users' ability to be free of unsolicited phone messages in 1991 when it added Section 227 to the Communications Act to prohibit telemarketing and unsolicited faxes to wireless phones and fax machines. I understand Margaret is going to talk a bit more on that.

To get back to the steps that wireless carriers have taken to filter Spam on the front end, there's some operational difficulties that are present in the wireless sphere that also distinguish us from the public internet. First, as I mentioned, for SMS text messages, carriers use the customer's phone number as the address. While in the past wireless carriers obtained phone numbers in 10,000 number blocks, and these were sequential numbers. For the last year, numbers are being assigned in blocks of 1,000. And with number portability, which is scheduled to take effect in November of this year, wireless numbers will be interchangeable with wire line numbers and vice versa.

Wireless carriers do not market their subscriber list to third parties. I'm not aware of third party lists that market wireless numbers. And as a result, wireless numbers are not posted throughout the internet. This makes it difficult, not impossible, but

difficult for Spammers to obtain addresses for unsolicited SMS messages.

So, just to recap, as an industry, wireless carriers know they need to protect their customers from Spam. They have the ability to monitor what people might be trying to do in assessing their network and the industry is doing everything it can to anticipate and minimize these problems before they become a service affecting problem that detracts from user's willingness to use wireless data services.

MS. HONE: Thank you, Mike. And just to be clear, we will take questions at the end of everybody's presentations.

Jim Manis has a PowerPoint presentation. And, again, Jim is the Chair of the Mobile Marketing Association.

MR. MANIS: And, hopefully, this PowerPoint will let me talk faster.

Just curious, while I'm bringing this up, I presume that the majority of the audience here carries a wireless phone. How many of you have ever sent a text message? How many of you have received a text message? And how many of those text messages have been something other than peer-to-peer or to an associate or a friend or family?

So, the Spam category that we're talking about is that last category, is kind of the non-peer-to-peer messaging traffic that we're seeing that we anticipate to take place. And I think Mike's comments here are clearly that. It's new and developing and, in fact, there are some gating issues that have still not been resolved to really accelerate the development of non-peer-to-peer messaging, particularly that type of messaging that would be branding related or fall into the mobile marketing category.

So, I guess size does matter in the case that as you see things like inter-operability and inter-carrier agreements come into play, a common short code agreement come into play, then you see a spiking of activity in peer-to-peer or non-peer-to-peer messaging. And carriers -- and in the case of mobile marketing, certainly well-respected national brands have a lot at stake in communicating to their subscribers or to their customers. And there is a great degree of consistency, if you will, in terms of taking strenuous measures to protect that.

So, earlier today, sitting in the audience was particularly useful for me to hear the concurrent debate coming on between e-mail and wireless Spam. Wireless mobile marketing is, in fact, very, very new. A lot of

the issues that have been discussed today and yesterday and tomorrow are issues that are down-road issues for mobile marketing, but are very serious issues that we take into consideration today.

Mobile marketing is two-way interactive marketing using a mobile message platform of SMS, MMS, which is a multimedia platform that's coming into play today in the United States, also in Europe and in Asia, and it is direct and interactive with the consumer. And it involves a variety of things. It involves everything from sweepstakes trivia questions, polling primarily through things that you've seen recently with AT&T and American Idol; for example, coupon offers, et cetera. This is nothing particularly different from the debate that you're having with respect to e-mail.

But it is about -- because of the unique nature of it, because of the personalized nature of mobile marketing, where you're sending something to a handset that we carrier around, that we all feel very passionately about protecting intrusive type behavior. It is a channel, a media channel that does generate, and the value of it does generate customer loyalty. So, behavioral aspects around that are designed to encourage loyalty; therefore, measures to prevent Spam are critical.

It also is uniquely qualified to provide the consumer additional controls to protect their own access to information, if you will, whether it's internet access or whether it's simply access that they go out and grab for whatever purpose. So, there is a value there.

Mobile marketing, itself, we define as an association, with the Mobile Marketing Association representing wireless carriers, major brands and vendors, as something that has to provide value to the consumer. There has to be some reason why you have a mobile marketing campaign, whether that value is entertainment or trivia value, which is a bit segmented based on who's using mobile marketing. For example, you can appreciate that perhaps a teen segment market might be particularly interested in a trivia type exchange around a movie property and they would see value in that entertainment prospect.

Or a different segment, perhaps in the 30s and 40s, might be interested in collecting a specific mobile coupon for a specific product discount at a specific store location in order to save 25 percent right now on this particular product that I want.

So, the industry is one, if you go back to Mike's comment with respect to where we're going on this hockey stick, has not taken off yet, but is scheduled to

take off, primarily because of a number of gating issues in the process of being resolved. Analysts today predict that the mobile marketing industry will be an industry that will peak out at about $8 billion. It's certainly active today in Europe and Asia.

You're seeing a substantial type of activity. You're seeing a range of activity, some of which was undertaken incorrectly, some examples which provide us with a learning here in North America and examples that relate to Spam, because if there's anything that will kill this from developing and sustaining over a long period of time, it is the introduction of Spam. So, it is a threat. And as both CTIA and MMA and other industry associations proceed in responsible development of this industry, there are things that we are trying to take into account.

So, the MMA, again, as an organization representing an industry in a developmental stage, is in the process of putting together policies for agreement with -- between carriers and brands and technology vendors, and our initiative, basically, is focused on two types of things. One is establishing an industry code of conduct that provides principles for companies that are engaged in this behavior to follow, best practices and things of that nature.

Also, the second element of this is enforcement and that enforcement initiative is focused on a certification process, a verification process that, in fact, some companies are abiding by that code of conduct and technology elements that focus on both opt-in and opt-out principles.

A code of conduct really provides the consumer with choice. This has to be in every element, an opt-in -- and I don't want to get into the semantic conversation that occurred in the last panel. Let's just focus on the principles here because that's what's important to us and we can find the terminology as we wish, but nothing will occur without you, as a user of your wireless device, wanting that information on your phone.

And secondly, you will be given control that after you opt-in to opt-out either at the end of that campaign or after any other database that you're in. So, those are both opt-in and opt-out principles, as well as constraint. There's unique technology parameters that allow you to set the number of messages that you would like to receive. Part of the value of this activity is to enter into a dialogue between the brand and the consumer. So, there are constraint prospects for a code of conduct that set the number of dialogue that you would engage in.

Same thing with customization consideration, if you will, with respect to the value that you need to receive as a consumer and, of course, confidentiality. Mobile marketing sits uniquely between the wireless carrier and the national brand and both of those entities have very strong and passionate concerns about protecting their subscriber or protecting their consumer, and that code of conduct has to acknowledge and allow for that.

So, the second aspect of this initiative is the enforcement initiative and that's broken down again, as I mentioned, in three different categories. One is the certification or the verification that a company that's engaged in this activity abides by the code of conduct that is published and agreed to by the industry itself. And that industry is representing a wide range of players.

And then, secondly, is the development of the technology tools that allow for those controls. In this case, of course, is the opt-in databases, a national opt-in database that would be appropriate for some segments of the population, and as well as an opt-out database that would be integrated with that to allow opt-out on any given exchange that takes place or on a life span basis.

So, this particular industry is viable. It is

one which has some unique value to all parties involved, including consumers, and it is one which every aspect of -- every player in this particular industry is today, at the very early stages of this industry development, very concerned about making sure that it's done correctly and avoiding issues that we've seen around the world and certainly avoiding the issues that we've seen with e-mail.

So, I thank you very much for your attention. I'd be happy to address any questions that you have.

MS. HONE: Thank you, Jim. Our next speaker is Jiro Murayama, who is from NTT DoCoMo and will talk about the experience in Japan with wireless messaging generally and their Spam problem.

MR. MURAYAMA: Thank you very much. I would like to appreciate FTC for organizing this kind of event and also including DoCoMo in this panel.

Again, my name is Jiro Murayama and I work at the Washington, D.C. office of NTT DoCoMo. So, I've been here in D.C. for about one-and-a-half years, so please, nobody worry about SARS.

(Laughter.)

MR. MURAYAMA: Today, I would like to talk about Spam problems to wireless in Japan. First, I will introduce the wireless industry and DoCoMo and then I

will get into wireless Spam problems and how we have been dealing with and --

MS. HONE: Jiro, can I interrupt you for just a second?

MR. MURAYAMA: Yes.

MS. HONE: It's a particular problem up there that you need to be close to the mic.

MR. MURAYAMA: Okay, sorry about that. Then legislative and legal measures taken to fight Spam in Japan.

NTT DoCoMo is Japan's largest and leading wireless communications services in Japan. We offer i-mode, which is wireless internet service and the world's first 3G service. On the screen, you can see some of our latest handsets that we offer in Japan. Those built-in camera type handsets are especially popular as users in Japan can send and receive pictures and videos attached to an e-mail.

Now, I'd like to introduce our i-mode service which is a little bit in detail because it is deeply related to wireless Spam problems in Japan. As of March of this year, the number of mobile phone subscribers in Japan is approximately 75.6 million. Among them, DoCoMo has close to 44 million subscribers. And i-mode service has attracted nearly 38 million subscribers since its

launch in February of 1999. So, about 85 percent of our users subscribe to i-mode.

There are several reasons for this success. One is rich content. Because of the business model in the language which is called a compact CTML, it was easy for content providers to offer i-mode sites. Currently, there are close to -- there are more than 67,000 sites for i-mode.

Second reason is various online services, just like access via internet, e-mail, purchasing something, reserving hotels, airline tickets, anything you can think about that you can do over the internet.

Third reason is low fee of about $30 a month and since it uses a packet switching system, meaning users are charged for data they send and receive, it kind of creates an always connected environment.

As you can see, our i-mode service has been extremely popular. This popularity, in turn, has unfortunately generated great interest from Spammers in Japan.

So, let's get into the heart of our topic. E-mail addresses for i-mode uses user name@nttdocomo.nejp. Please imagine that AOL had about 35 million users worldwide. I think that's as of June 2002 and i-mode now has close to 38 million users. So, there are 38 million

users with the same domain names.

Initially, user names before at-mark (phonetic) were their phone numbers. So, all Spammers had to do was create an 11-digit numerical user name which was very easy and cheap for them. Our initial response to this was to encourage users to change their user names to whatever they wanted, including alphabetical words. However, these Spammers then developed a software that generates a combination of random digits or alphabets that could be utilized as an e-mail address to send bulk e-mails.

These figures are as of October 2001, but in one day, 150 million normal e-mails and Spams reached users and 800 million were returned since they did not exist at that moment. Those returned e-mail had an enormous burden on our e-mail server which resulted in a delay of e-mails. And Spams reaching users are, of course, very annoying to most of our users, but on top of that, as I mentioned in the last slide, because we charge users from data they send and receive, they have to pay for receiving Spam.

Let me now introduce measures that we have been taking to fight those Spams, two aspects on our side and one legislative measure. One is customer protection. As I said, we promoted heavily on encouraging users to

change address and now 90 percent of our users have changed their address. Also, as of October 2001, 54 percent of all users received zero Spam a day. But as Spammers are going more and more ingenuous and were able to create more accurate mailing lists, as they know which ones were valid addresses and which ones were not used, about 30 percent users still receive one to five Spams per day and about 4 percent of them receive as many as 30 Spams a day. We also instituted a program to reimburse users for charges they incurred on receiving Spam.

The second aspect is technical measures. We began a measure such as to limiting incoming e-mail to only user-specified addresses and domains and blocking user-specified addresses. We also added new function in network, on blocking any e-mail sent to large numbers of invalid e-mail addresses and blocking fake domain e-mails. This measure not only eliminated heavy burden on our server but also inhibited the ability of Spam senders to generate lists of valid addresses.

Also, we introduced new handsets that enabled users to check the subject line of an incoming e-mail prior to downloading. The users now can choose not to receive the e-mail and simply delete it.

The third aspect is the legislative measures. These are the two laws that were implemented in July of

last year. Both laws require to indicate unauthorized advertisement on the title, sender's name, address and e-mail on top of the message body and e-mail address for opt-out. They both prohibit sending e-mails to users who have opted out. The first law, it prohibits sending by unknown e-mail address produced by Spam software.

In reaction to this law, we began taking measures to blocking any e-mail containing the unauthorized advertisement. After the warning then the respective government body will go through a series of steps of investigation in order, a violation of any of these steps will consequence in fine or possibly even imprisonment.

Now, I would like to introduce two litigation cases in Japan. In October 2001, there was a preliminary injunction to prohibit sending commercial bulk e-mail to dating site Spammer. They had been sending as many as 900,000 bulk e-mails generated with random e-mail user names, which resulted in delay of e-mails. Even after we gave warning, they kept on sending Spam. So, we requested for injunction.

The other cases, the company had been sending a total of four million Spams in two months. We brought an action against the company on the basis of violation of contract for our service for legitimate internet

marketers.

So, have these measures been effective? First, because of privacy of communications, which is guaranteed by Japan's constitution, it's been difficult to take legal measures against Spammers to this point. And up to now, measure taking has not gotten as far as just sending a warning. So, right after the laws went into effect or we take any measures, the number of Spams decreases. But from around November of last year, Spam started to increase again. And Spammers are fully aware that they are illegal and they continuously send Spam without appropriate indication or valid return e-mail.

There are some positive signs looking forward. We are encouraged with the latest litigation and we will continue our litigation against malicious Spam senders. Also, according to a research by one Japanese media, the Spam industry seems to be in an oligopoly state, meaning a technically savy company or individual that has updated mailing lists is sending Spam on behalf of multiple concerns. We see this as an indication that we have been taking measures that's making it more difficult for Spammers to succeed.

The number of entities that are sophisticated enough to continue sending Spams have been narrowed. This, in turn, we hope will make enforcement actions more

effective. Also, number of Spams in other normal e-mails reaching users decreased from 150 million as of October 2001 to 90 million as of March of this year.

So, in conclusion, as data traffic over wireless network continues to grow, so will Spam and Spam to wireless is likely to become a social problem in the U.S. as well. We all need to understand that Spam is a potential problem on wireless networks, not just fixed. And in the Internet world, Spam is predicted to soon exceed 50 percent of the e-mails being sent, but as for DoCoMo, that percentage is far above the net figure and DoCoMo is and continues to lead an aggressive fight to control the Spam problem in Japan.

Lastly, from our experience, not only legislation and regulation, but also measures by carriers are also important. Therefore, there's a need for stronger global coordination between regulators and carriers for addressing the problem of wireless Spam. Thank you.

(Applause.)

MS. HONE: Thank you very much. Our next speaker will be Rodney Joffe who will tell us a little bit about his experience with wireless Spam and his litigation.

MR. JOFFE: Thanks, Lisa. I guess at the

beginning, I should start with a bit of background. I've been a card-carrying member and a dues-paying member of the Direct Marketing Association for 20 years. So, I come from the marketing side. I've also been involved in computing for 25 years, and in 1994, I was the founder of a company that some of you know called Genuity, which I sold to GT in 1998.

But in 1994, we really began to look at the issues of Spam. The very first e-mail Spam occurred in the beginning of 1994. And as a group, we sat by, looked at the Spam, talked about it and said that it was a very bad thing, as typical academics and scientists, and we debated whether it was right or wrong and in what way it was wrong. And while we did that, Spam took off and we were unable to put the genie back in the bottle.

The costs were enormous from an ISP point of view and I looked through that in 1996 and 1997, along with most of the other ISPs. There's always been this assumption that e-mail is free and the internet is free and it truly isn't. The costs are enormous in terms of server infrastructure, in terms of sys administration to handle those, and it has to be borne by someone. And it can't be borne by the senders, unfortunately; it's borne by the recipients.

In 2001, in January of 2001 -- and I have to be

cautious and just preface my remarks, you're aware of already that there is litigation pending, so I'm only going to talk about the facts related to the case I'm involved in. I received a text message to a cell phone. As you all know, when you get a message on your cell phone, it's not like e-mail. You can ignore the e-mail, you can set it aside for once a day. But when you get a message on your cell phone, by definition, it's immediate and it's urgent and you look at it. And that's one of the benefits and I recognize the benefits.

However, that particular message was addressed to someone I had never heard of and I assumed it was a message that had been sent to me by mistake. I called the company involved and told them I had received the message and they thanked me profusely for letting them know and they said they'd get the message to the correct person. I thought nothing more of it until about two months later when I got another message also talking about mortgages and the fact that the mortgage rate had dropped, once again addressed to someone other than myself.

Before calling the company, I happened to mention it in a meeting with some of my staff who all have cell phones from AT&T in the same 10,000 block. Each one of the employees had received exactly the same

message. At that point, I began to realize that this wasn't an error.

I probably would have ignored it like most people -- most people you talk to in terms of e-mail and say, why didn't you just hit delete, it's simple. But having lived through what occurred in 1994 and having understood how difficult it was to move things back once it had grown legs, I was determined not to allow it to become something that killed the benefits of cell phones and small message services on cell phones. And so, I filed an action.

The only avenue available to me was to actually file under the TCPA, which I can thank Margaret for, is a federal statute that governs telemarketing as well as sending of junk faxes and I filed suit in small claims court, which is the only court you can really file in for both messages, which allowed me to file for $1,000. I don't make a living out of the $500 judgments; however, I wanted to try and do everything that I could to make sure that I stopped it as early as I could. Now, understand, this is now January of 2001. So, it's over two years ago.

In that particular case, the case was moved from a justice court by the company that I filed suit against to the superior court. And at that point, it is

something that I'm no longer able to handle myself, that requires counsel, and I engaged counsel in the case.

The status of the case currently is the defendants in that case asked the court for a motion for summary judgment to dismiss the case. The trial court turned that down. The case was then appealed to the Arizona State Appeals Court, certain parts of it, and the appeal was turned down about a week ago. So, it's back to the trial court. So, the current status is that the case will be heard some stage in the next six or seven months in Arizona.

I guess an easy segue to Margaret is to say that it's not been easy to find legislation. The TCPA, when it was first introduced, I don't think that SMS and messaging to cell phones was something that anyone envisaged. It would be very helpful if there was a clear way of allowing individuals who receive cell phone Spam to actually take advantage of the private right of action, which is the key part of the TCPA, and allow individuals, like myself, to make it much more different for cell phone Spammers to send Spam.

In my case, it was done through AT&T, the use of a cell phone number together with a publicly known domain and there's no easy way to stop it. You know, I appreciate the fact that there are filtering techniques,

but I know something about filtering techniques of e-mail and I can tell you that the Spammers are very good at bypassing them and the rest of my staff have continued to receive Spam over the last two years.

The day that I filed suit against this particular company was the last time that I received any kind of unsolicited advertising to my cell phone. I've had the same number for a number of years. What I will say is, yesterday evening, I received my first cell phone Spam in two-and-a-half years. It happened to be from a company offering international advice on long distance rates for telephones and it had a California phone number to call back. As you know, there is a California law on the books now that prohibits it.

So, it may be starting up again and it may be becoming a problem once again. Hopefully, it's not going to get that much worse.

MS. HONE: Thank you, Rodney. And just for those of you in the room who aren't familiar with the TCPA, that's the Telephone Consumer Protection Act.

The next group of our panelists are going to -- are limiting their remarks to two or three minutes, three or four minutes depending, so that the audience has a chance for questions. So, thank you to our first four panelists for really covering the gamut for us so that we

could get to our commenters, and by way of introduction, we're not expecting a symposium from Margaret on the TCPA. She is one of our commenters and we've restricted her to a few very moments of comment.

MS. EGLER: Thank you, Lisa. The TCPA, Telephone Consumer Protection Act, let me just talk a little bit about that. That would indicate why the FCC would be at this panel, and we were very happy to be invited. So, thank you.

The Telephone Consumer Protection Act is actually -- you can't thank me. It was passed 12 years ago. But even though it was passed 12 years ago, it had specific protections for consumers when they receive unsolicited faxes, when they get telemarketing calls that are prerecorded or auto-dialed, when those calls come to them during certain periods of the day, et cetera, et cetera. I'm just going to talk about one small part of it, although we do have an open proceeding, a very big open proceeding going on right now on telemarketing and a proceeding we're working closely with the FTC on, as a lot of you probably already know.

But as far as the TCPA works, in terms of wireless devices, the TCPA prohibits any call to any number assigned to a cellular device or a pager that is done using an auto-dialer or includes a prerecorded

message. So, that's an important thing to know. It's a call done to a number assigned to a wireless device. So, basically, if it's done -- whether it's done from one cell phone to another cell phone or from a regular land line phone, basically, if you're dialing in a number and it's going to a cell device or a pager and it's using an auto-dialer, which most of the -- you know, what we call Spam or telemarketing calls are done using auto-dialers, that would be prohibited.

But before you get excited about it, the way we would read that is that would just be calls that are made using the number to the device. We would just consider that probably a violation under the TCPA.

What we have not reached is the question of when it's sent to a cell device and it's an Internet address. So, it would be, you know, lisa@ftc.gov or even the phone number at Skytel.com or whatever that is, that's different than going to a number assigned to a wireless device. And we haven't reached whether or not that would actually be something that's covered by the TCPA.

So, to understand that and to understand what Rodney went through in Arizona, the interesting thing about the TCPA, Section 227 of our act basically allows three different types of jurisdiction almost. It

basically lets the FCC to create rules. It allows the states to also create rules that can be more restrictive, as long as they're not inconsistent with ours.

So, it allows enforcement actions at those two levels, but it also allows for private rights of action, which is why you'd find Rodney in the small claims court in Arizona making these claims and this happens for all TCPA violations all over the country. So, there's a lot going on and so there are lots of different jurisdictions that could be saying lots of different things.

As far as what we've seen at the Commission, we have not seen a lot of complaints on wireless Spam. We have not seen things come in in the type of numbers that we've seen in, say, for example, wire line telemarketing or slamming, which are two of our biggest topic matters. So, that's sort of the FCC view and what's going on with us on this.

MS. HONE: Thank you, Margaret. Our next panelist is Andrea Blander. She's filling in, so some of you will have Wally Hyer listed on your agenda. Andrea was good enough to fill in when Wally couldn't make it. She's Corporate Counsel with AT&T Wireless and she focuses her work in the privacy arena, but has a broad understanding of the topic here today.

MS. BLANDER: My affectionate name at the

company is the Czarina of Privacy and for others in the company, the less affectionate term is the acronym COP.

I think as a carrier, the Spam issue is one of trust and confidence for our customers. We want our customers to be able to use us SMS, we're encouraging them to adopt it, and to the extent that they find they're getting SMS on their phones, it's going to be a problem for us.

We've learned from the foreign experiences, as you've heard, we have filters in place, and we have been aggressive in the instances where there have been Spam incidents on the phone. Another way that we help our customers is they are not charged for incoming messages on our phones.

So, we're working on solutions. We've learned from the online world. But we're in a position more like an ISP in the wired world. Spam is bad for us. It uses network resources. It will prevent people from using SMS. But on the other hand, we also need to communicate with our customers and we like to use SMS as one of those methods. So, we're a little bit concerned about legislation at this point. The technology is still pretty new and we don't want anything coming out that's so broad that it impacts our ability to communicate with our customers.

In addition, it's different than e-mail. Strict SMS has a limit of 160 characters. So, in terms of providing opt-out opportunities, you are more restricted in what you can do.

MS. HONE: Thank you very much, Andrea. Our next two panelists are both mobile marketers and they both have experience here in the United States and abroad. So, first is Marc Theermann with YellowPepper.

MR. THEERMANN: Thank you. Carl and I maybe stand on the other side of the fence a little bit and, of course, while Spam is a horrible thing and it will hurt the industry, so companies like ours are doing everything to prevent it. Our company, in specific, provides a wireless marketing platform that lets other companies send and receive text messages.

So, I just want to highlight two instances where a company that does everything right would appear to be sending out Spam. Basically, there's two types of Spam. The first one is an unwanted message from a known source, and that could occur that a consumer has opted in to receive messages either to a billboard or website or maybe even a television ad. And the truth is, there's two ways of how they could have opted in and then received a message that they don't want anymore.

The first one is, the number could have been

reissued. So, for example, if I'm an AT&T customer and I cancel my contract with AT&T, my number will be reissued to another individual within a certain amount of time. So, there could be instances where you would receive a text message from a company that you don't know because you have not signed up for the service, but somebody else has signed up for the service and there would be no way currently for the marketer to know this.

And the second way is that sometimes you have forgetful consumers. We ran a campaign for a large portal in Europe where people signed up to receive marketing messages and in one particular instance, we had a consumer that was so angry that the call got escalated to me and they threatened to sue us and said, you are sending me messages that I never signed up for. So, we went to the system together and I looked him up in the database and I could see the time and day when he signed up with this mobile phone number. But, of course, there is a chance that it wasn't him that signed up.

So, I said, do you maybe happen to have a teenager in the household, and I heard him scream in the background, Jason, come over here, there's somebody on the phone that wants to ask you something.

(Laughter.)

MR. THEERMANN: So, Jason promised that he did

not sign up for the messages, which was true, but I saw that the password in the account was Jason. So, the consumer had obviously signed up with his son's name, even as the password, so it was pretty clear that he did sign up for the messages, yet he had either stopped wanting those messages or forgot that he ever did sign up.

So, I think those are two instances, A, a reissued number, and secondly, the forgetful consumer, where the marketer is doing everything right, yet it appears that he's Spamming the person. So, we need to find ways of how to protect companies that engage in good marketing. And I think we all agree that one of the biggest chances of doing that is a very, very easy opt-out process. There's nothing worse than getting a message that you can't opt-out of. So, if the opt-out process is easy and good, I think that should be one of the strongest defenses against Spam.

MS. HONE: Thank you, Marc. Carl from Telemedia.

MR. GUNELL: I think that the difference between the internet that you have on your desktop and the internet you have on your telephone is that there is a business model for the mobile internet. The recording industry made more than $71 million last year from the

ring tone business in Europe, which would indicate that the business is sort of in the excess of $750 million, just selling legal content.

So, the reason we haven't really seen it in the United States yet is because until very recently there was a number of disperse networks that could not communicate with each other and the handsets were incapable of using the more sophisticated content, which is changing very rapidly.

Another thing is that, talking about e-mail and e-mail addresses being telephone number at a wireless carrier, with all the new handsets that are in the stores today, the camera phones and the color phones, it's completely possible to configure those to receive the same e-mail that you are on your Outlook in the office or any other mail client. So, there isn't really a distinction anywhere between wireless internet and the internet. You will be able to -- I download my mail on my phone. I think 70 percent or so of whatever e-mail I receive is Spam. So, it's very important to not treat the wireless world separately from the fixed line world because the Spam issues will affect the wireless even more simply because there is an ability to charge for content, which is very, very appealing.

And much of what the music industry -- I mean,

their business model in the hardware world is dead and if you think about it, there isn't really a format after the CD. It will be digital transfer. And the mobile telephone, the way it looks today, is an ideal device to download content to, if it's an MP3 file or some other proprietary format. And what they're seeking is the one-to-one relationship with the customer. They want to know the name of the person that likes that particular artist simply because they want to communicate with them.

And the same sort of ties in to all this location-based advertising, which we haven't even seen yet, where you're sort of driving through an area and there's a Starbucks in that area and they're sending out a message to you offering you 10 percent off of the next cup of espresso.

If you think about it, in the west, we already have a location-based system because it's not like in Europe where the area code of the mobile telephone indicates what carrier you have. Here, you know, if you're making a phone call or your mobile phone is a 202 area code, you can assume that that person is in Washington, D.C. So, on a very broad level, it's already possible to do some kind of location-based advertising.

So, I think what we need to address -- I think it was this gentleman who received Spam in the past.

What we need to do is to focus on issues where the users can opt-out of further information in a very easy fashion, because there's going to be an enormous amount of Spam and there's really no way that you can prevent it technically. It's very possible to emulate person-to-person messages simply by buying a SIM card and using GSM mode. It would look to the operator like it came from another individual.

So, I don't really believe in technological solutions. I believe in organizations that work together on a global basis because most of the Spam will come from countries outside of the U.S. and can address this opt-out issue. Thank you.

MS. HONE: Thank you, Carl. And our last panelist is Al Gidari from Perkins Coie.

MR. GIDARI: Thanks, Lisa. You know, Carl's exactly right. The very distinction between a wireless telephone and a computer has disappeared. And to actually separate out a panel on this is actually a little bizarre today because it's the same set of issues. It just happens over a different network with a multitude of different network operators and people that interact with it.

The real problem is that there is jurisdictional uncertainty. We don't know who regulates

it. We have 30 states now with legislation that define a computer broad enough to include a cell phone. But certainly none of the restrictions in those statutes about what has to be in an unsolicited e-mail to be legal apply to a 160-character message. So, we have uncertainty about what state laws apply.

Even trying to apply those laws to a telephone which doesn't understand borders, which doesn't identify a user other than whose hand it happens to be in, and where the facilities happen to serve more than just one jurisdiction. The switch could be in New Jersey serving New York as, indeed, in the AT&T wireless network it is, and in other carriers' networks as well.

So, we no longer have a clarity of jurisdiction.

It's also enjoyable to see the FTC and the FCC up here, together, asserting jurisdiction over the same thing. I can't imagine there's a single wireless carrier out there that understands or believes SMS is regulated by the FCC under the TCPA. They're all looking inside messages today to filter them and we can't do that if it's a telecommunications service, legally.

So, all the lawyers, go send your client updates and I think you'll get a bunch of new clients tomorrow giving them advice on what is or isn't legal. That's a huge problem and it doesn't get any better when

you think about the globalization of the service because we truly are in an era of convergence, where carriers now facilitate these communications, and whether they're e-mail, SMS or phone communications, wherever the user wants to go and travel.

The business models are not clear. The transactional uncertainties, really, I think create a hindrance to rolling out the service. It's not the fact that you might get Spam, it's actually now the fact that somebody might regulate you out of business tomorrow by changing the character of what that service actually is. And so, I think clarity would be a good thing one way or the other and that would help carriers immensely. Thank you.

MS. HONE: Thank you all. Now, I have about 20 questions I want to ask myself and I understand why my fellow moderators chose the question and answer format. But I promised questions from the audience. So, if you start to flag, I have questions. But questions? Right here.

A mic is coming to you. And if people could remember to identify themselves.

MS. BLAKELY: Hi, I'm Carrie Blakely (phonetic) from Forbes. I'm sorry, I'm going to mispronounce your name, Jiro, since you seem to be sort of in the future

and I had no idea that it was still so prevalent and so heavy over there, the wireless Spam. We talked earlier about the chilling effect that this was having on business and the internet, you know, people are just scared to buy things online. They didn't, you know, want to have to have seven different e-mail boxes and stuff and even legitimate marketers were having problems, and it was chilling their business, and they weren't getting response rates.

Are you seeing that with what could be described as legitimate mobile marketers over there? Are they having a chilling effect because of all this Spam?

MR. MURAYAMA: Yes, I think they are. I think the legitimate internet marketers also want to send a certain number of e-mails, but I think they are more or less affected by the Spammers in Japan. And one of the services we offer is provide for those legitimate internet marketers the lasting connection with our server so that they can send bulk e-mails who have opted in for their service. So, yes, it is -- they are affected by the Spammers and we are, also, taking measures for those legitimate internet marketers to offer a legitimate service.

MS. HONE: Actually, Rodney Joffe, one of our panelists, has a question and I'm going to let him go

ahead and ask it.

MR. JOFFE: I guess it's aimed towards the company's that are involved in SMS and electronic marketing now, cell phone marketing. One of the fundamental issues is that -- a real issue with Spam is this ability for senders to shift the cost to the recipients. I know that AT&T said that they don't charge, but I know that if I asked if I could have a cell phone account that only received SMS messages, there would be a charge associated with that if I wasn't taking anything else. So, there is a cost involved, the same as there is in e-mail.

I'm real interested, if I wanted to opt out from receiving cell phone messages, would I opt out once and never again receive a cell phone message I didn't ask for or are you suggesting that I should do it legitimate marketer by legitimate marketer?

MR. THEERMANN: I can start. Well, the question is, again, where did you first opt into the marketing campaign? So, we've got to assume that somewhere -- let's not talk about illegal Spam where somebody generated your number and sent you something. But we're talking about you opted in at some point and now you want out. Then I think you should opt out of that specific campaign for sure.

I think one of the main distinctions, and this is where, I think, wireless is different than internet, is that the opt-in is actually so much easier because we can't forget, we're talking about a wireless device, so you can opt-in everywhere, which means you could see a poster on the street that says, you know, get your new ring tone, send a text message to the system and so forth, which means that any time you interact with your cell phone, you could potentially opt-in to something that you don't know.

So, if you would opt-out of everything, you would opt out of the entire network, so to say, and you couldn't really interact anymore.

MR. JOFFE: I think an interesting thing with that then is that what you are not starting to see is some of the legacy of what happened in the e-mail world because I don't believe that anyone in the e-mail world or the anti-Spam community has any issue with companies that send e-mail that's been asked for.

But what's happened is a backlash. You have so many people that assume that they get one bite at the cherry or one bite at the apple, that you react to everything. And if the kind of thing you're talking about in the cell phone world is -- and your definition of a legitimate marketer is someone who has an actual

active assertive way that someone opted in and that that should continue, I don't believe you'll find anyone in the anti-Spam community that argues in anyway.

On the e-mail side, we've heard a number of panels over the last couple of days where people talked about the fact that I am a legitimate marketer because I've got bricks and mortar and I sell regular products and I believe that my products are important for you and I don't see why I shouldn't send mail to you.

So, I think that in the cell phone world, you should differentiate very carefully when you talk about legitimate marketers because in the e-mail world, and on those panels, to them, legitimate marketers are people that sell products and those that are illegal are people that sell products that are not the products that they sell. There's no definition in terms of whether it's really illegal. It's someone else's product. And if you listen to Bob Winston from the DMA, that's the kind of message you heard for a couple of years.

And I know that Jerry Cerasale is over here. It's been -- we're legitimate marketers, we've got a normal business and we send you mail. I think it's wonderful that that's your definition and make sure that you publicize it. Because if you don't, you'll be painted with the same brush as the legitimate e-mail

marketers.

MS. HONE: And there's a question over here.

MR. GUNELL: Can I make some comments to that, if you don't mind?

MS. HONE: Okay.

MR. GUNELL: We keep talking about two things here. We have sort of the SMS text messaging marketing and then you have your e-mail marketing and there's -- you're going to receive e-mail marketing and there's nothing really that companies like us can do about that.

On the SMS marketing side, I think that there will be the establishment of trusted third parties. What I mean by that is, that if we take the reality television shows, for instance, like American Idol, it will be beneficial to American Idol to make an arrangement with a company who connects you to all six major networks instead of just AT&T, because obviously that will generate more traffic and more one-to-one relationships.

So, you will find there will be a number of companies who will be connected with all the majors and they will also, naturally, then be sort of a gateway to consumers from brands they wish to advertise.

So, where would you opt out? You would opt out through a trusted third party.

MR. JOFFE: Where would I have opted in, though

--

MR. GUNELL: Well --

MR. JOFFE: -- to those six companies I didn't know about at the time I got my cell phone?

MR. GUNELL: Well, ideally, what's going to happen is that there will be sort of unique short codes that are networked across network. Otherwise, it's not going to work from sort of an advertising standpoint.

MR. JOFFE: But how would I have identified the fact that I'm prepared to accept messages from a TV show that doesn't exist at the time I get my cell phone?

MR. GUNELL: Well, you're going to be invited to vote on the TV show, right? So, you're --

MR. JOFFE: So, I didn't opt in?

MR. GUNELL: No, no, no, no, no. You're not receiving the advertising to your telephone. It's part of the television programming. So, do you want to vote for a particular candidate or do you want to vote for a particular issue, what you do is to send a message to this in this short code. When you've done that, your memory's been captured. And there might be sort of a privacy policy, say, that by voting you also agree to receive messages regarding a long distance service or whatever it might be. So, you would go back and you would opt out from whoever facilitated the message.

MR. JOFFE: I'll buy that.

MR. GUNELL: All right.

MS. HONE: Okay. There's a question over here.

MR. CROCKER: Thank you. Dave Crocker, Brandenburg Inter-Networking. I think it's great to have a panel like this. Wireless is interesting and it's a different kind of experience from internet mail. But what occurs to me is it takes a long time to make laws, that laws are expensive, that other procedures take a long time and that they're expensive, and that we want to be careful about having too many different efforts focused too narrowly, and that the view that SMS messaging is somehow importantly different from internet mail and that the kind of Spam in the one is somehow interestingly different from the Spam in the other strikes me as leading one down a very wasteful path.

Yes, SMS is low bandwidth right now and, yes, the devices it goes to tend to be small resources. But, in fact, low bandwidth and limited resources are true. Often internet mail in some places, and oh, by the way, the ones that are limited resources now and limited bandwidth are getting higher bandwidth and more resources.

So, let me strongly suggest that you represent a very important exemplar of certain kinds of traffic and

activity, but that the real differences, the deep differences probably are non-existent. For example, just by way of an example, the idea that somehow it's easier to opt in with phones rather than internet mail is just plain not true.

MS. HONE: So, is your question, do the panelists agree with that?

MR. CROCKER: Yes, thank you.

MS. HONE: Anyone in particular want to handle that?

MR. THEERMANN: So, how would you opt in into an e-mail campaign in the subway or with a magazine?

MR. CROCKER: Oh, I'm sorry. You were raising the issue about mobility and the answer is? I don't use SMS, I use internet mail and it will work in some subways, though not much in the Metro here.

MS. HONE: Right. So, what you're speaking to is the concept of convergence that I think all of our panelists have touched on in one way or the other. But there are some differences still. There's a question way in the back.

MR. COGILL: My name is Gary Cogill. I'm an attorney from New York. I have a question about the slide on how it's very important for everyone to read privacy policies when you opt-in for some service. If

I'm on a handset and I'm opting into a service on the handset, what's -- I guess maybe the question to Mr. Murayama or the person from AT&T -- are you going to post a privacy policy to the handset or are you going to encourage the user to go to a website later on to read a privacy policy?

MS. BLANDER: It's interesting you ask that. We're actually involved in a project with Trustee to come up with some guidelines for the wireless world because there are those technical limitations and we're trying to develop some guidelines about what is a way to provide reasonable notice to customers on a phone and what is a way to give them meaningful choice. So, I don't know that we have an answer for you today, but that we are working on it because it's obviously an important issue.

Jim, this speaks to some of your issues. Did you want to address it?

MR. MANIS: Yes. That is in the process of being developed, but the norm today is to refer back to the website.

MR. ALTSCHUL: If you go to each of the national carriers' websites, you'll find privacy policies associated with their service descriptions.

MS. HONE: There's a question right here in the middle, if there's a mic.

MR. FOX: Hi, Jeff Fox, Consumer Reports. The question of geographical marketing and the scenario that I've heard raised a few times of you're driving down and the Starbucks or the Home Depot sort of reaches out and touches you and says, you know, come on it, a little Orwellian, I think. It seems to me to raise some real significant privacy questions. I was trying to think about how it might worked, and either you've opted in with Home Depot and Starbucks ahead of time, in which case the cell phone company which is tracking your location through the towers is somehow informing them that you're in the neighborhood, which raises questions about whether you want these companies knowing where you're going and when you're going. You know, they've got computers and they can track you.

If you haven't done that, does that mean that the cell phone companies have standing orders to sort of beckon to everyone who wanders through this particular part of the highway, in which case that seems to me to be Spam or really an unsolicited kind of offering? So, really, the question is, how would this work and what are the privacy implications?

MS. HONE: Let me just start by saying, your question involves a whole lot of interesting issues; in particular, the location information is something that

everyone on this panel has been grappling with in one form or another. But we are focusing on unsolicited wireless e-mail. So, to the extent that people want to address the question, I would ask you to focus on the unsolicited portion or the marketing portion and to the extent location information sort of adds a veneer to it, it's interesting and useful, but I don't want to use this panel to get into a deep debate over location information and the carrier's responsibility, the marketer's responsibility, that sort of thing.

MR. ALTSCHUL: But, Lisa, there is an important thing to note about location information. It's one of these things that there ought to be a law and there is a law. In 1999, Congress, as part of a statute in 9-11, passed a law that establishes active consent from a wireless user to use location information. That's very different than other non-location based kinds of services.

MS. HONE: That's right and that's part of what makes it that much more complicated. Do our marketers have any thoughts or Andrea on location information and text messaging?

MR. GUNELL: I think sort of in the Starbucks scenario, the most likely solution will be that you're driving by a billboard and you're sending information --

you contribute your telephone number somehow and they send you back a graphic picture, which is probably some kind of a bar code that can be scanned in the store and now they know where you live.

MR. MANIS: Yeah, the Starbucks example was kind of overly used and abused. That just simply won't happen. What will happen is exactly that. So, if you're on the road and if you're changing locations, if you go by a billboard, there will be a short code advertised on that billboard for a discount at the Starbucks which is located at the next exit. So, you access that texting in the short code to your telephone and then you receive back a coupon that when you pull off, you redeem for whatever.

That's how -- you're not going to -- because of the privacy issues here and the location-based issues here, you're not going to just simply be roaming and getting offers to your handsets.

MS. HONE: And you do that all while driving very safely.

MR. MANIS: Yeah, thanks.

(Laughter.)

MS. HONE: Was there somebody down here who wanted to add anything?

(No response.)

MR. CLARK: Jonathan Clark, Open Wave Systems. The claim was made from one of the panelists that filtering wireless messages was actually not legal in the U.S. because these were regulated under the TCPA and, hence, under common carrier, or at least what I understand to be common carrier.

I'd like to ask the representatives from AT&T and the FCC whether they consider this to be the case and whether the answer is different for SMS versus electronic mail, as Mr. Crocker brought up?

MS. HONE: I actually think the panelists said that they thought -- Al, was that you or --

MR. ALTSCHUL: That was me.

MS. HONE: -- was that you, Mike?

MR. ALTSCHUL: I think a number of us touched on it. My statement is --

MS. HONE: I'm sorry, I think you actually had it backwards, so that's why I'm asking them to clarify.

MR. ALTSCHUL: Yes. My statement was that a text message can be filtered because it's not a common carrier service that falls under a definition of an information service because it's a store and forward message.

MS. EGLER: Yeah, I mean, right now, that's definitely Mike's interpretation of what information

services and I'm not an expert on information services. But there is a difference. There's telecommunications, there's information services. But then there's this thing called telephone calls in the TCPA and in the TCPA, basically Congress said it's any call to a wireless number. And because they use the examples of cellular phones and pagers and pagers have -- even though this is a 12-year-old statute -- has only ever had to do with text, then we wouldn't differentiate between voice and text.

So, what I'm saying is that if you're using a wireless number, okay, and you're going to a wireless device and you're using an automatic dialing system or a prerecorded message, that would be considered a violation of the TCPA. That's different than whether or not it's a telecommunications service or an information service. Does that make sense?

MR. ALTSCHUL: Well, I don't find in the TCPA authority for carriers to filter. TCPA gives --

MS. EGLER: Right, that's what I'm saying. We're talking about two different things.

MR. ALTSCHUL: -- the user a right of action against the person sending the unsolicited message.

MS. EGLER: Right, right. That's what I'm saying. The TCPA is sort of a special statute in that it

reaches all telemarketers, which isn't our -- the FCC's usual group, but we have jurisdiction over everybody because of the TCPA. The question about what's a telecommunication service versus what's an information service doesn't come from the TCPA.

But the content of a telephone call being made to a wireless number is something that comes out of the TCPA.

MR. GIDARI: I sure hope there are no class action plaintiff lawyers in the audience.

MS. HONE: May I ask a point of clarification, Margaret? So, if I get text messages on my phone number at my wireless carrier, does the at my wireless carrier take it out of the telephone number?

MS. EGLER: Yes, yes, and I want to make that -- I think I was pretty specific about that when I first talked, but let me just reiterate that. What we're talking about is a wireless number, a number assigned to a wireless device, and that's what the TCPA is limited to. So, that's sort of the hypothetical that we're dealing with is, you know, the text message to the cellular device using a wireless number that's assigned to a wireless device; it's not an e-mail address, it's not your wireless number at AT&T or even your e-mail address.

Our Commission has never reached the question of whether or not an e-mail to a wireless device would come under the TCPA. So, that's really important for people to understand that.

MS. HONE: And can I ask our panelists who know better than I, does anyone receive text messages that way or is it always your phone number at your carrier?

MR. ALTSCHUL: No, peer-to-peer messages from one wireless device to another or from one wireless network or another just use the traditional telephone number to address the message.

MS. HONE: Thank you.

MS. EGLER: And that would be the TCPA.

MR. JOFFE: Could I ask a technical question there as a computer scientist? If I was to set up a telephone system, a regular wire line telephone system that had the ability to allow me to remotely program as a forwarded number, a cell phone number, and I did that in a highly automated way, the fact that I'm dialing a wire line number, with a prerecord, and it's being translated by a piece of equipment in the wire line system at my office and dialing a cell phone number, am I violating the TCPA in that way?

MS. EGLER: Well, I guess the first question is, just to make sure we're all talking about the same

realm, are you using internet addresses at any point here, e-mail addresses?

MR. JOFFE: I'm making a telephone call to a wire line number which is not illegal under the TCPA.

MS. EGLER: To a wire line number.

MR. JOFFE: The wire line number has an automated system of actually each time I dial the same number, it increments a cell phone number by one, makes the call and it's actually that automated process that's doing that.

MS. HONE: So, you've created the software that does that?

MR. JOFFE: It's trivial software.

MS. HONE: But you're purposefully using it with the theory --

MR. JOFFE: Yes, correct.

MS. HONE: -- that you'll try and circumvent the TCPA?

MR. JOFFE: Correct, absolutely. Because the use of the e-mail address at a domain which is then going through a switching mechanism at the central office of AT&T Wireless and is then saying that that e-mail address is actually this telephone number, is a way of circumventing the TCPA in much the same way. And I have to believe if that's the case, then there are probably

1,000 telemarketers that have suddenly said, aha, I can avoid any prosecution under the TCPA because I'm calling a wire line number, I'm not -- there's a mechanism that's doing it automatically. It's not my fault.

MS. HONE: And we thank you, Rodney, for suggesting that.

(Laughter.)

MR. ALTSCHUL: So, Rodney, the Spam that you received previously was sent to your telephone nubmer@attws.com, is that correct? Mobiled to att as opposed to a text message sent to your phone, is that right?

MR. JOFFE: Right.

MS. EGLER: So, then, that takes it out of the hypothetical. As soon as we have the at whatever, basically we've never reached that question, whether that's covered under the TCPA. What we're talking about specifically -- and this is why I told you not to get too excited about it. What we're talking about specifically are the numbers, the actual numbers that are assigned to the wireless devices, and that would come under the TCPA, not that are numbers that are part of an e-mail address and then that --

MR. ALTSCHUL: So, there is delivery of text messages today that way?

MS. EGLER: Yes, there is.

MR. ALTSCHUL: And we have defined the peer-to-peer text messaging for the interoperability among wireless carriers as a message that's coming from a mobile device. So, using a wire telephone device with a wire telephone number would not pass through the gateway, not pass through the SMS interoperability gateway, at least.

MS. HONE: There's a question in the back. Can you please identify yourself?

MR. BAKER: Philip Alan Baker, VeriSign. First, I just got a wireless Spam selling me the secret to solving Spam. So, should I just reply to it and, you know, we don't need to do anymore?

But the other question was, what happens when the telephone system and the internet collide in that in a very short time, the basic infrastructure that we're going to be using for doing our SS7 (phonetic) messaging is going to be the same infrastructure that we use to support the DNS? So, these distinctions have been made that, hey, it's going on the wire line, it's going to a telephone number and, oh, it's got an at sign in it. Those distinctions aren't going to mean very much in maybe a few more months. So, what happens when there is that convergence? Has anybody been looking into it?

MS. HONE: Al, do you want to answer that question?

MR. GIDARI: No.

(Laughter.)

MS. HONE: Not because I think he's been looking into it, just because I think he's the clean-up hitter.

MR. GIDARI: But that's my point. These regulatory structures just don't apply and to try to stretch an old law to meet new technology produces the business uncertainty that makes everybody afraid of those that are sitting up here and those that are the class actions lawyers and that add tremendous transaction cost.

And it's a real problem trying to stretch these statutes to reach behavior that is absolutely bizarre when you realize the TCPA does not cover a live person calling a cell phone to market any product or service. It's just not covered. It's not regulated. Only if it's auto-dialed with a prerecorded message.

You're paying the cost of the phone call. I get them all the time from brokers and other people that get my name through some other list, and it's just not regulated. Yet, an SMS message would be? I mean, it really absolutely is a crazy structure.

MS. EGLER: Just a slight correction. It's

auto-dialed or with a prerecorded message.

MR. GIDARI: Sure. But that broker sitting there at his desk dials away all day long at a number range that he's picked up from some third party, the same way you would generate a 10,000 block list.

MS. HONE: So, Al, are you recommending national legislation?

MR. GIDARI: I'm not recommending a thing.

(Laughter.)

MS. HONE: There's a question all the way in the back.

UNIDENTIFIED MALE: Globen from Mail Frontier. This was more targeted toward Mr. Murayama, but somewhat to the panel in general. Mr. Murayama mentioned that NNT DoCoMo is partnering with some or providing a service to some legitimate marketers to market to users. I'm wondering how you go about making that definition, how you actually verify if they come and say, this is a completely double opt-in, super-confirmed list, how you go about verifying and authenticating that process?

MR. MURAYAMA: I'm not exactly sure about how they're going to verify that particular internet marketer as legitimate. But I would believe that there is a certain level of requirements that we require for each of those internet marketers. For example, I don't think

DoCoMo and the internet marketer is merely exchanging those information by e-mails, for example. So, they have valid address, they have valid e-mail, for example.

There would be a certain level of requirements to get into that service. That's what I would believe.

MS. HONE: And there's a question way over here.

MR. GERARD: Sorry, it's another question. My name is Philippe Girard from the European Commission in Brussels. Just to tell you that we have this kind of problem of convergence and we have a new directive in place since last year where we have the same system, by the way, it's an opt-in system. But anyway, we've tried for a converging solution to that. So, we have an opt-in system for all sorts of e-mails and that covers, of course, SMS and MMS and normal e-mails, et cetera.

MR. ALTSCHUL: If I can say just one quick note. I think Carl alluded to this earlier. It is developing a little bit differently here in the United States where the carriers are essentially -- there will be a pool of aggregation companies who will perform a variety of services, perhaps the most important of those services will be to protect content in Spam.

MS. HONE: And before we end, did any of our panelists have anything else they wanted to add or any

other questions you wanted to ask of each other that you didn't get a chance to?

(No response.)

MS. HONE: Well, then I'd like to thank all the panelists for participating and thank you to the audience for staying. I hope this was helpful and useful to you. We certainly found it informative.

(Whereupon, at 5:14 p.m., the hearing was adjourned.)

C E R T I F I C A T I O N O F R E P O R T E R

MATTER NUMBER: P024407

CASE TITLE: FTC SPAM PROJECT

DATE: MAY 1, 2003

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the notes taken by me at the hearing on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED: MAY 20, 2003

SONIA GONZALEZ

C E R T I F I C A T I O N O F P R O O F R E A D E R

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

SUSANNE BERGLING