

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

FEDERAL TRADE COMMISSION

I N D E X

INTRODUCTION	PAGE
BY MS. HARRINGTON MCBRIDE	4

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

FEDERAL TRADE COMMISSION

IN THE MATTER OF: )  
CAN-SPAM REPORT TO CONGRESS. )  
 ) Matter No.:  
 ) P044405  
 )  
-----)

WEDNESDAY, JULY 20, 2005  
Room 238  
Federal Trade Commission  
600 Pennsylvania Avenue, N.W.  
Washington, D.C. 20580

The above-entitled matter came on for  
conference, pursuant to agreement, at 1:05 p.m.

1 APPEARANCES:

2

3 ON BEHALF OF THE FEDERAL TRADE COMMISSION:

4 CATHERINE HARRINGTON-MCBRIDE, ESQ.

5 MICHAEL DAVIS, ESQ.

6 ALLYSON HIMELFARB, INVESTIGATOR

7 CELIA WASHINGTON, Intern

8 600 Pennsylvania Avenue

9 Washington, D.C. 20058

10

11 ALSO PRESENT VIA TELEPHONE:

12 RAY EVERETT-CHURCH, Privacy Clue, LLC

13 ANNALEE NEWITZ, EFF

14 CHRIS HOOFNAGLE, EPIC

15 DEB FALLOWS, Pew Internet

16

17

18

19

20

21

22

23

24

25

## P R O C E E D I N G S

- - - -

1  
2  
3 MS. HARRINGTON-MCBRIDE: Thank you all very much  
4 for joining us on the call today. This is one of a  
5 series of interviews that the FTC staff are conducting  
6 with knowledgeable folks who have something to say about  
7 Email and the Can-Spam Act.

8 Our interview today is with privacy  
9 professionals, and we very much appreciate your taking  
10 the time to talk with us. As you all know, this is a  
11 continuing dialogue, one that began even before the  
12 Can-Spam Act was passed, but we very much appreciate  
13 your willingness in the last year and a half to let us  
14 know your thoughts and to provide us data.

15 It's very helpful to us, as we complete our  
16 mandate under the Act, to create the various reports for  
17 Congress that we are called upon to do.

18 I would like to go ahead and begin the call with  
19 a somewhat odd formality, given that there are only four  
20 people joining, beyond those of us here at the FTC, but  
21 we would like to take roll, because this is going to be  
22 a transcribed call. Deb Fallows, from Pew Internet, are  
23 you with us?

24 MS. FALLOWS: I'm here.

25 MS. HARRINGTON-MCBRIDE: Great. Thank you, Deb.

1 Chris Hoofnagle from EPIC?

2 MR. HOOFNAGLE: Hi, I'm here.

3 MS. HARRINGTON-MCBRIDE: Hi, Chris. Annalee  
4 Newitz from EFF?

5 MS. NEWITZ: I'm here.

6 MS. HARRINGTON-MCBRIDE: Hi, Annalee. Has Ray  
7 Everett-Church joined us? Hopefully Ray will be able to  
8 join in in not too long.

9 Here at the FTC, again I'm Katie  
10 Harrington-McBride. I'm working on this project and  
11 have worked on some others on CAN-SPAM, and with me  
12 today are my colleagues Mike Davis, an attorney also  
13 working on this project with me, and an intern of ours,  
14 Celia, who will be here for only a few more days, but  
15 who has been very helpful in helping us get our data  
16 together to complete our report to Congress, so we're  
17 glad to have her here.

18 In December 2003, as you all know, Congress  
19 enacted and the President signed the Can-Spam Act which,  
20 among other things, directs the FTC to report on the  
21 effectiveness and enforcement of the Act. Our report to  
22 Congress is due by the middle of December 2005.

23 Most of you will recognize that that means that  
24 Staff has to complete its research and compilation of  
25 data much earlier than that, so we appreciate you taking

1 time out of your summer afternoon to talk with us.

2 We've been gathering data since the passage of  
3 the Act, base line data on Email and spam and  
4 information since the passage of the Act about how  
5 effective it has been and our enforcement statistics  
6 under the Act.

7 This interview with privacy professionals will  
8 be transcribed for the public record and will be part of  
9 the record for the report to Congress, and this  
10 interview is just one of several ways that the FTC is  
11 currently seeking information that will be relevant for  
12 the report on effectiveness and enforcement.

13 Because today's call is being transcribed for  
14 the record by a court reporter, who is listening to the  
15 call, it is very, very important that when you wish to  
16 speak, you begin by stating your name and your  
17 affiliation. For example, this is Katie  
18 Harrington-McBride with the FTC. It's such a small call  
19 I think first names will probably suffice.

20 If you don't remember, a team of us will swoop  
21 down on you and let you know that you've forgotten to  
22 identify yourself. We want to have a clean record for  
23 this, and so the call will just proceed more efficiently  
24 if you make a note of this now. Don't worry, if you  
25 forget, we will absolutely remind you.

For The Record, Inc.  
(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555

1           Finally, and just to be absolutely clear, your  
2 views expressed here today will be transcribed for the  
3 record and may be appended to the report to Congress or  
4 otherwise made public, just so everyone is clear on  
5 that.

6           Are there any questions before we begin?

7           MS. FALLOWS: Katie, this is Deb Fallows. I  
8 actually would not describe myself as a privacy  
9 professional. I can give you some other way to describe  
10 me, but I am happy to stay on this call, but privacy is  
11 not my particular area of expertise.

12           MS. HARRINGTON-MCBRIDE: Okay. No, that's a  
13 very fair critique, and I should say when we were  
14 compiling these calls, there certainly are some places  
15 where we blur some lines, and so I apologize if the  
16 characterization is incorrect, but we would very much  
17 appreciate it if you would stay on the call and  
18 contribute.

19           We know you're very knowledgeable in this area,  
20 and although we've incorrectly denominated you, if you  
21 don't mind sticking with us, that would be great.

22           MS. FALLOWS: That's fine. It's probably an  
23 enhancement to my reputation.

24           MS. HARRINGTON-MCBRIDE: Fair enough. We've  
25 just allowed you to branch out. You'll be consulting in

1 no time.

2 Any other questions?

3 Let me give you a little bit of an overview of  
4 what we're going to try to accomplish today here in this  
5 call. We're going to cover four main topics, and these  
6 will not surprise you if you've looked at the Can-Spam  
7 Act lately or if you ever indeed looked at it because  
8 we're very much following along in a methodical way and  
9 trying to parse through the Act and study its  
10 effectiveness provision by provision.

11 The first questions that we'll address will  
12 relate to any marketplace developments or technological  
13 changes since the passage of the Act in December of 2003  
14 that may affect the practicality or effectiveness of the  
15 Act, and we'll talk more in depth about this. I want to  
16 kind of you give the overview, but just to stimulate  
17 your thinking initially, this could include, but  
18 certainly is not limited to, changes in filtering  
19 technology, methods of authentication, the new or  
20 increasing use of non traditional devices for receiving  
21 Emails, such as hand-held devices or cell phones, so  
22 that's the first area we'll touch on.

23 The second will be the extent to which the  
24 international transmission of Email may affect the  
25 effectiveness of the Act and any suggestions you may all

1 have for changes.

2 The third topic we will address is how  
3 consumers, particularly children, can be protected from  
4 obscene and pornographic material, and we'll talk there  
5 about our quote, unquote, Brown Paper Wrapper Rule  
6 mandated by the Can-Spam Act and other possible  
7 technological solutions, and finally, we'll go over in  
8 some detail the specific provisions of the Act, and  
9 we'll talk about their effectiveness and enforcement.

10 For each of these four main areas, I'll ask a  
11 series of questions. My colleagues here at the FTC may  
12 also ask questions, and if any questions occur to you  
13 while we're talking, I would like to keep this a fairly  
14 open dialogue.

15 We wanted to try to make this minimally  
16 burdensome, so we did not invite you here in person to  
17 enjoy our humid afternoon in Washington. I know some of  
18 you get to benefit from that naturally, but because  
19 we're on the phone and it won't be possible for us to  
20 see your body language suggesting that you want to  
21 speak, we'll just have to try to be as attentive as we  
22 can. If you have something you would like to say, just  
23 speak up, and if we need to cue people up at that point,  
24 we will.

25 When you are called on, if you could just state

1 your name and the organization you're with and provide  
2 your answer, that would allow us to best get the record  
3 in order, and with that, I'll begin with our first  
4 issue, and that is whether there are any marketplace  
5 developments or technological changes since the passage  
6 of the Act that may affect the practicality or  
7 effectiveness of the Act.

8 I guess that's the ubber question that is asked  
9 by Congress in the Act. I guess we have thought about  
10 it in some detail, and specifically I guess my first  
11 question would be: Are there new or increasingly used  
12 methods for receiving Email that consumers use, such as  
13 cell phones or hand-held Email devices, and has this had  
14 any affect on the effectiveness or the practicality of  
15 the Act?

16 MS. FALLOWS: Katie?

17 MS. HARRINGTON-MCBRIDE: Yes.

18 MS. FALLOWS: Are you looking for answers just  
19 from us?

20 MS. HARRINGTON-MCBRIDE: Absolutely, that would  
21 be great.

22 MS. FALLOWS: This is Deb Fallows. I'm from the  
23 Pew Internet Project, and what we do and probably what  
24 we bring to this conversation is nationwide polling of  
25 Internet users about various aspects of the Internet,

1 behavior awareness, attitudes and so forth, so I would  
2 say what I'm going to bring to you is more fact figures  
3 than recommendations, although you could draw some  
4 implications from them.

5 MS. HARRINGTON-MCBRIDE: We love data, so thank  
6 you.

7 MS. FALLOWS: Okay. Certainly one of the things  
8 that we've seen in the last year and are starting to  
9 measure is Internet accessibility through things that  
10 aren't tied to your desktop, mobile devices of all  
11 sorts, and I was just actually reading today that there  
12 are now 800 million cell phones in use or registered  
13 around the world.

14 Of course a lot of the new ones have  
15 availability for text messaging, and we have a figure  
16 that's probably let's say, I think I can check this for  
17 sure, from '03, that 17 percent of people have accessed  
18 the Internet through mobile devices of one sort or  
19 another, and that number is growing.

20 It's growing, it's something that we're going to  
21 be measuring more, but I think anyone would say this is  
22 the wave of the future, that people will carry around  
23 their Internet access with them and not be tied to any  
24 place in particular.

25 So from our point of view, new forms of Internet

1 access may mean opportunity to spam of different sorts,  
2 involving new technologies, and new ways around existing  
3 anti-spam impediments.

4 The other thing we're seeing is spam coming in  
5 instant messaging, that that is certainly on the  
6 increase. I don't know if either spam delivered to  
7 mobile devices or the instant messaging spam are covered  
8 by the Act, but they should be because they're out there  
9 and certainly growing.

10 That's a starter thought.

11 MS. HARRINGTON-MCBRIDE: That's very helpful to  
12 have that background information and to know you are  
13 tracking that. Does anyone have any further data or any  
14 input on whether the fact that it may be now even more  
15 common to access your Email through a mobile device has  
16 any affect on the practicality or effectiveness of the  
17 Act?

18 MR. HOOFNAGLE: This is Chris Hoofnagle from the  
19 Electronic Privacy Information Center.

20 MS. HARRINGTON-MCBRIDE: Hi, Chris.

21 MR. HOOFNAGLE: Hi. I would just note that in  
22 some cases, subscribers are paying a bandwidth fee for  
23 information they receive on mobile devices, so when they  
24 do receive spam on their wireless phone or Sidekick,  
25 there are cases where the individual is paying a

1 bandwidth fee for each one of those messages.

2 MS. HARRINGTON-MCBRIDE: So there are real costs  
3 associated with this?

4 MR. EVERETT-CHURCH: This is Ray Everett-Church.  
5 I'm sorry I joined late.

6 MS. HARRINGTON-MCBRIDE: Hi, Ray. Thanks for  
7 joining.

8 MR. EVERETT-CHURCH: I just would add that due  
9 to interface constraints on many mobile devices, it can  
10 be more difficult to access things like unsubscribed  
11 links and to see all of the data or information about  
12 the origination of the Email. In some cases if the  
13 Email message is particularly heavily formatted with  
14 special text, colors and graphics and such, it can be  
15 very difficult to navigate an unsolicited commercial  
16 Email message in order to take advantage of what  
17 opportunities CAN-SPAM gives you to unsubscribe, even  
18 assuming that the Email is compliant.

19 MS. HARRINGTON-MCBRIDE: Ray, this is Katie. I  
20 just want to jump in quickly because those were actually  
21 some follow-up or what you've said reminds me of some  
22 follow-up questions that I had intended to ask.  
23 Anecdotally we have heard the same thing, that is, that  
24 if you access your Email through a wireless device, it  
25 may be difficult or impossible to access opt-out links.

1           Is there any hard research on this or any  
2 studies that have been done that quantify this in any  
3 way that we should be looking at or incorporating into  
4 our report?

5           MR. EVERETT-CHURCH: This is Ray Everett-Church.  
6 I'm not aware of any studies of that nature, but I just  
7 know anecdotally from my own personal experiences in  
8 using mobile devices to access Email that it's more  
9 common than not that heavily formatted Email messages  
10 are difficult to navigate through using mini wireless  
11 devices.

12           MS. NEWITZ: This is Annalee from the Electronic  
13 Frontier Foundation. I just wanted to add to this point  
14 that because of the fact that people are now going to be  
15 accessing Email from mobile devices, this is driving  
16 more people to use sort of web-based Email services  
17 because they're going to want to access the same Email  
18 from many different locations at once.

19           And I think the fact that they are using these  
20 web-based services is going to underscore Ray's point  
21 that there's going to be a lot of HTML formatting that  
22 they may not have access to.

23           The other thing that I think we might want to  
24 talk about is that I think that this puts the ball in  
25 the court of the ISPs or the web mail services to be

1 filtering their mail, filtering out spam and going  
2 certainly beyond the scope of CAN-SPAM in order to give  
3 their customers as spam-free an experience as possible,  
4 and I think that's where we run into a lot of issues  
5 around how do these companies filter out mail that may  
6 not be spam, how are they trying to kind of go beyond  
7 the law to please their customers, and I think that that  
8 is also an issue, because I think CAN-SPAM kind of has  
9 been a legal informatory for the companies to say, Look,  
10 we're not going to deliver certain things, and this is  
11 going to enhance your experience, but as a user, you may  
12 not have much control over what you get in your mailbox  
13 now.

14 MS. HARRINGTON-MCBRIDE: Okay. Thank you.

15 MR. HOOFNAGLE: This is Chris Hoofnagle again  
16 from the Electronic Privacy Information Center. If I  
17 may amplify Ray and Annalee's point regarding opt-out  
18 links that lead to pages that can't be navigated by  
19 wireless devices, this problem is probably going to be  
20 exacerbated by the adoption of rich media on the web  
21 sites of the various marketing companies.

22 When I say that, I mean that many of these  
23 companies are now using themes or animations that cannot  
24 to read on a wireless phone because they are too  
25 complex, so opt-out processes may be affected by the

1 inclusion of such rich media tools.

2 MS. HARRINGTON-MCBRIDE: Would that also be a  
3 problem for access from the desktop?

4 MR. HOOFNAGLE: This is Chris from EPIC. The  
5 problem continues to exist if an individual's desktop  
6 did not have so-called rich media software, whether it's  
7 Macromedia's Flash or the capability of handling Java or  
8 JavaScript. We are big advocates of using clean HTML  
9 because it is compatible everywhere and anyone can use  
10 it, but we're seeing the big increase in the adoption of  
11 rich media on the various marketing sites that may not  
12 be compatible with everyone's devices.

13 MS. HARRINGTON-MCBRIDE: Okay. That's helpful.  
14 One of the --

15 MR. HOOFNAGLE: If I may.

16 MS. HARRINGTON-MCBRIDE: I'm sorry, go ahead.

17 MR. HOOFNAGLE: If I may add one more thing.  
18 This is Chris from EPIC. We noted on direct costs  
19 earlier, that is the cost of bandwidth to the  
20 individual, but I think it's also important to pay  
21 serious attention to the amount of time and frustration  
22 that recipients of spam endure.

23 My spam filter captures 7,000 messages a month.  
24 If I were to spend my time reviewing those messages, it  
25 would take me many hours, and at my hourly rate, that

1 could be a lot of money.

2 A lot of other consumers are in this position  
3 where their time, which is very valuable, is being  
4 wasted sorting through spam, so I think that  
5 individual's time in handling spam should go into the  
6 calculus when considering the costs of this type of  
7 marketing.

8 MS. HARRINGTON-MCBRIDE: All right. Thank you.  
9 One follow-up question. This is Katie at the FTC again.  
10 We touched on this I think a little bit in something  
11 that either Chris or Ray had said, and it is this: In  
12 addition to the potential difficulty with opting out  
13 through a mobile device, are there also limitations  
14 because of the size of the screen of these mobile  
15 devices that might impact the disclosure requirements,  
16 I'm thinking specifically of the requirement that you  
17 have a truthful header, and that is if your header is so  
18 truncated because of the amount of space you have, can  
19 that be problematic, and also the subject line, which  
20 again must be non-deceptive under the Act, and even in  
21 the specific instance of our Brown Paper Wrapper Rule,  
22 that is the rule we promulgated to address how sexually  
23 explicit Email should be labeled, there's a labeling  
24 requirement there that runs more than 20 characters?

25 Is that going to be something that would

1 necessarily be viewable on these mobile devices, or are  
2 there issues with that?

3 MS. NEWITZ: This is Annalee from the Electronic  
4 Frontier Foundation. I actually think that the concern  
5 about headers and subject lines may not be as pressing  
6 when you're looking at mobile devices as some of the  
7 stuff Chris was talking about, which has to do with the  
8 body of the message and having media in the body of the  
9 message.

10 So I think certainly if you have a tiny screen,  
11 it may be harder to read a subject line, but that's just  
12 part and parcel of having a very tiny screen, so I think  
13 that that may not be as much of a concern as sort of  
14 lots of HTML or lots of media.

15 MS. HARRINGTON-MCBRIDE: Okay. Thank you.

16 MS. FALLOWS: This is Deb from the Pew Project.  
17 I would chime in here to say that it's been our  
18 experience that the more sophisticated users are the  
19 people who are going out into the new gadgetry.  
20 Identifying the subject line is something that most  
21 people say they kind of look for if they're trying to  
22 identify spam, but I would wager a guess that the  
23 sophisticated users don't rely on subject lines as much  
24 as others do in identifying something as spam.

25 They're just more likely to be able to tell at a

1 glance and get rid of something they think is spam. So,  
2 subject lines are not as important to that user group in  
3 this case.

4 MS. HARRINGTON-MCBRIDE: Okay. Thank you.

5 MS. FALLOWS: I also have one additional data  
6 point for you. In March of 2004, we found that  
7 41 percent of Americans had used wireless devices like  
8 laptops or cell phones and so forth that are capable of  
9 accessing the Internet. We had found that 17 percent of  
10 them at that time said that they had actually gone ahead  
11 and accessed the Internet using those wireless devices.  
12 So you've got twice as many people who are capable of  
13 accessing the Internet wirelessly, and that certainly  
14 will be something that people, as they become more  
15 familiar with these devices, will start to do. So the  
16 numbers should probably rise pretty quickly.

17 MS. HARRINGTON-MCBRIDE: Great. Thank you.  
18 Anything else on new or increasingly used methods of  
19 receiving Email and their potential affect on the Act  
20 and its effectiveness?

21 MR. HOOFNAGLE: This is Chris. I have a  
22 different technical question to raise.

23 MS. HARRINGTON-MCBRIDE: I'm sorry, who is it?

24 MR. HOOFNAGLE: This is Chris from EPIC.

25 MS. HARRINGTON-MCBRIDE: Chris, thanks. Sorry.

1           MR. HOOFNAGLE: I just wanted to highlight this  
2 development that we think is new since CAN-SPAM, and  
3 that is that the list brokerage industry has established  
4 an ECOA database, that is Email Change of Address  
5 database, in order to track people down once they've  
6 changed Email addresses.

7           It is the case that many users, to escape spam,  
8 periodically change their Email addresses, and this  
9 database is a new technical measure that may frustrate  
10 individual's attempts to escape spam. ECOA database is  
11 being run by Experian, the credit agency.

12           On its web site it claims that it has  
13 100 percent opt-in, but for the life of me, I don't know  
14 what consumer would give their Email address to  
15 Experian.

16           MS. HARRINGTON-MCBRIDE: That's interesting. Is  
17 the access to this then fee based?

18           MR. HOOFNAGLE: I'm sorry?

19           MS. HARRINGTON-MCBRIDE: Is it accessed on a fee  
20 basis so that you would pay Experian to access this  
21 database and run a list of addresses against the change  
22 file?

23           MR. HOOFNAGLE: I believe this is what's known  
24 as an enhancement product that allows a company to send  
25 a consumer database to Experian, at which point Experian

1 adds, scrubs or deletes information from the company's  
2 database and then Experian sends it back to the company,  
3 so I think it's an enhancement service, and I imagine it  
4 is for a fee, but I do not know what the fee is.

5 MS. HARRINGTON-MCBRIDE: Okay. Thank you.

6 The next questions that I have, we're still on  
7 the first topic, that is marketplace developments or  
8 technological changes, certainly there was Email  
9 filtering before the passage of the CAN-SPAM Act, but  
10 you hear more and more about it and its efficacy, and I  
11 wanted to ask whether any changes or enhancements to  
12 Email filtering might have affected the practicality or  
13 effectiveness of the Act.

14 MS. NEWITZ: This is Annalee from EFF. I wanted  
15 to talk again about the issue of large ISPs filtering  
16 Email. There have been a lot of developments in this  
17 area. Most of the large companies like Hot Mail or AOL  
18 are constantly adding new technologies to sort of their  
19 complete anti-spam breakfast, as they like to put it.

20 One of the things that we deal with at EFF all  
21 the time are activist groups that are confronting the  
22 issues around having their Email blocked by a large ISP  
23 which can be very damaging if they're a group like Move  
24 On, for example, which is trying to organize a  
25 nationwide campaign that may only have a few days to be

1 effective, like if they're trying to influence a  
2 Senator's choice on a bill or something like that.

3 So actually just in the last month, we've had  
4 two large activist groups, one of which was Move On and  
5 one of which was a gay and lesbian group, that came to  
6 us having problems with ISPs that had added new filters  
7 in and were suddenly blocking all Email from these  
8 groups, and they had hundreds of thousand of members  
9 that they were trying to reach.

10 The problem that we have been seeing with this  
11 is that companies like AOL, for example, say that they  
12 will offer a white list for groups that are nonprofit  
13 groups that are sending lots of bulk mail, and that once  
14 such a group has sort of met their criteria of being a  
15 legitimate group and not a spammer, that their Email  
16 will go through, and we're seeing more and more that  
17 these white lists are no longer being honored and are no  
18 longer working.

19 And these activist groups that had been on the  
20 white list are feeling tremendous frustration, that they  
21 can't get a straight answer, that there are no federal  
22 guidelines. There are no even sort of policy guidelines  
23 about how such a white list would work, so they can't  
24 come to their ISP and say, Well, look here's how a white  
25 list should work for a group like us, once we're on the

1 white list, we're happy to be rechecked on a regular  
2 basis, but to be pushed off the white list again and  
3 have to go through the whole procedure of speaking to  
4 all of the reps that they have to talk to, it's  
5 tremendously difficult, and as I said if they're working  
6 on a campaign, what this can mean is tremendous losses  
7 for their group or tremendous difficulties in reaching  
8 their members in a particular area.

9 So these problems are continuing, and I think as  
10 we get new anti-spam filtering in place, we're going to  
11 see this more and more, and we're going to see more  
12 groups calling out for some kind of guidelines, some  
13 kind of carve-out, which will explain how a white list  
14 might work within a context of an anti-spam regime.

15 MS. HARRINGTON-MCBRIDE: Okay. Thank you.

16 MS. FALLOWS: This is Deb from the Pew Internet  
17 Project. I don't have a direct comment on what you  
18 asked about, but it's certainly been my experience in  
19 trying to keep up with the marketplace developments,  
20 that there are three of areas for anti-spam that are  
21 moving very quickly and very broadly. One of course is  
22 filtering and all of the different kinds of tweaks  
23 they're doing to it.

24 One is the authentication and Email sender  
25 identification. And another one is, something that I've

1 heard of, that's kind of a throttling of spam. It's  
2 effectively slowing down the channel or narrowing the  
3 tube, identifying spam upstream and slowing it down from  
4 reaching the targets shifting it back to the sender so  
5 that they have to go through a couple different steps  
6 back and forth before it actually transmits.

7 The reason I'm saying all this is that the  
8 breadth and scope of the new technology that is underway  
9 at this time is impressive, and that would suggest that  
10 the laws should be written broadly enough to include not  
11 only what you know about now, which I'm sure you get  
12 from all of your technology experts, but what is yet  
13 unnamed and going to be coming in the future.

14 MS. HARRINGTON-MCBRIDE: Okay. Thank you. Any  
15 other thoughts on filtering and its effect on the  
16 effectiveness of the Act?

17 MS. FALLOWS: This is Deb again. I have one  
18 other thought about filtering, and this goes back to the  
19 users again. All of our data shows that users are  
20 really quite naive in trying to set their own filters.  
21 So anything that can be done for users that can protect  
22 them rather than having them to have to install and  
23 apply their own filters is a good thing for a vast  
24 majority of the user population who aren't  
25 technologically adept enough to do that for themselves.

1 MS. HARRINGTON-MCBRIDE: Okay.

2 MS. FALLOWS: Or at least it should be made  
3 simple enough so that it's just a click of a button  
4 rather than having to fiddle around with a lot of other  
5 clicks and choices.

6 MS. HARRINGTON-MCBRIDE: Deb, this is a question  
7 for you specifically because I think this may be  
8 something that you've touched on in your research. Do  
9 you have anything that shows to what extent consumers,  
10 when selecting an ISP, look at their filtering  
11 capability?

12 MS. FALLOWS: I don't have any direct data on  
13 that. We just know that a lot of people will say that  
14 they're using filters, but we suspect when they say  
15 they're using filters, they mean that they have an ISP  
16 that applies filters for them. So it's something that  
17 is important to them -- and particularly important if  
18 they're parents -- but I don't have any direct figures  
19 on that.

20 MS. HARRINGTON-MCBRIDE: Okay. Another  
21 development, not necessarily since the passage of the  
22 Act but it's gained some steam since then, is the  
23 process of developing an authentication standard that  
24 may help in slowing the tide of spam and allowing law  
25 enforcement agents to identify the source of spam, and

1 so I wonder if anyone has any thoughts about any new  
2 developments in authentication, any changes in that  
3 area, and how they affect the practicality or  
4 effectiveness of the Act?

5 MS. NEWITZ: This is Annalee from EFF. I just  
6 have a short comment, which is that it's fairly well  
7 known at this point that a great deal of spam is now  
8 authenticated, so unfortunately, it doesn't look like  
9 sender authentication is really going to do much to stop  
10 spam.

11 MS. HARRINGTON-MCBRIDE: Okay. Thank you.  
12 Anyone else?

13 MR. EVERETT-CHURCH: This is Ray Everett-Church.  
14 Let me just piggyback on that. Sender authentication  
15 all by itself is not likely to do much, and that's why  
16 it's so important that in future consideration of the  
17 role of authentication in dealing with the spam issue,  
18 that further attention be paid to then adding to  
19 authentication levels of accountability and some of the  
20 considerations for reputation systems and other factors  
21 that will make authentication more of a meaningful  
22 element.

23 Right now, you could authenticate yourself as  
24 being accurately emanating from a particular source, and  
25 that doesn't guarantee the source or the Emails

1 themselves are not spam, but with authentication comes  
2 the capability of authenticating to an individual or a  
3 responsible party and then holding that party  
4 responsible for any violations of law.

5 That's sort of the next step of evolution of  
6 authentication and something that I and others have  
7 spoken about in previous FTC events, including I guess  
8 the last workshop where in particular we were proposing  
9 the trusted Email open standard as one example of taking  
10 authentication to that next step, to holding people  
11 accountable for failure to comply with the law, using  
12 authentication to tie people to their deeds and to hold  
13 them responsible.

14 MS. HARRINGTON-MCBRIDE: Okay. Thank you, Ray.

15 MS. NEWITZ: This is Annalee at the EFF again.  
16 I wanted to follow on to what Ray said and sort of  
17 reiterate some stuff that I said also at the Email  
18 Authentication Summit at the FTC, which is that one of  
19 our concerns at EFF is maintaining people's ability to  
20 engage in anonymous free speech. This is part of the  
21 First Amendment or part of the way the First Amendment  
22 has been interpreted in a number of Supreme Court  
23 rulings, and we're deeply concerned that if we have a  
24 regime of Email authentication where everyone's Email  
25 can be traced directly back to the actual person who

1 sent it, that it will really undermine people's ability  
2 to engage in free discussion of political issues.

3 It will undermine journalists' ability to do  
4 their work if they want to work with anonymous sources  
5 who are contacting them via Email, and so I think we're  
6 very concerned about looking toward a world where  
7 anonymous free speech is being squelched, so I just want  
8 to register that concern.

9 MS. HARRINGTON-MCBRIDE: Okay. Thank you. Any  
10 other thoughts on authentication?

11 This will apply not only to Deb, although it's  
12 her organization that I'll be quoting from, but to  
13 everyone. A recent study by the Pew Internet  
14 Organization found, and I'm sort of paraphrasing here,  
15 that while the volume of Email has increased since the  
16 passage of the CAN-SPAM Act, that the frustration of  
17 recipients has somewhat lessened, and I'm wondering if  
18 anyone has any comment on that finding, if anyone wants  
19 to offer interpretation or analysis.

20 MS. FALLOWS: Well, this is Deb at Pew, so since  
21 I wrote that, I should probably speak up first here.

22 MS. HARRINGTON-MCBRIDE: Okay. Fair enough.

23 MS. FALLOWS: People are saying that they are  
24 getting a little bit more spam in their inboxes. I  
25 would preface that by saying there is probably a whole

1 lot more spam out there, and just fractionally more  
2 that's actually getting to people's inboxes, so the  
3 filtering is actually rejecting a lot more of it than it  
4 was before. My sense of the decreasing frustration from  
5 people is based on a couple of things.

6 One is that they're just getting used to it, the  
7 same way you get used to going through security lines at  
8 airports or getting stuck in traffic jams. It's not  
9 something you like, and it's not something that you  
10 don't want to get rid of, but it's something that's  
11 becoming a fact of life, and people are just learning to  
12 live with it.

13 The other thing is that I think a lot of people,  
14 as they get more spam or have more experience dealing  
15 with spam, are getting a sense of some control over it.  
16 They develop their own little strategies for how they're  
17 going to deal with spam, and that sense of control also  
18 leaves them less frustrated. So you're getting used to  
19 an old problem and feeling like you can wrestle with it  
20 a little bit better than you used to be able to.

21 This is certainly not an interpretation that  
22 says spam is no longer a problem. It's just saying that  
23 with experience people are able to face spam with a  
24 little less hysteria than they used to.

25 MS. HARRINGTON-MCBRIDE: Okay. Thank you, Deb.

1 MS. FALLOWS: This is Deb again. I guess this  
2 is probably the point to introduce some new data that we  
3 have. When we first started studying spam at Pew, we  
4 were worried that the problem was going to become so  
5 grotesque that it would turn people away from Email  
6 entirely or at least to a large degree. We had some  
7 trends showing that from the few years before the  
8 CAN-SPAM Act until just after the CAN-SPAM Act that the  
9 number of disaffected emailers was actually growing.

10 Increasing numbers of people were turning away  
11 from Email. But our latest numbers show that this trend  
12 is reverting. So while spam is still causing people to  
13 use their Email somewhat less and turning them away from  
14 Email a little bit, it's not a figure that's rising.

15 MS. HARRINGTON-MCBRIDE: Okay. Thank you.  
16 Let's talk a minute about zombie drones where innocent  
17 user's machines are hijacked by spammers as a result of  
18 insecure connections.

19 Has the use by spammers of zombie PCs or  
20 networks had an impact on the effectiveness of CAN-SPAM?

21 MS. NEWITZ: This is Annalee with EFF, and I  
22 would just say that I think, going back to the sender  
23 authentication issue, if what you're trying to do is  
24 identify who is sending a particular mail and use that  
25 as a way to track down a spammer, obviously having a

1 zombie machine is going to make it more difficult  
2 because it's going to make it impossible to find out  
3 where the spam originated from.

4 MS. HARRINGTON-MCBRIDE: Right.

5 MS. FALLOWS: This is Deb from Pew. We've  
6 recently done a survey about Spyware and Adware that  
7 people have on their computers, and one of the  
8 interesting general findings of that is that most people  
9 have very little idea of how infected or threatened  
10 their computers are by things that can happen to them,  
11 and they don't know what they've got. They don't know  
12 how they got it. They don't know how to get rid of it,  
13 so it's an issue.

14 These findings just reflect how vulnerable  
15 general users are to this situation.

16 MS. HARRINGTON-MCBRIDE: Okay. Thank you. Some  
17 of the press reports suggests that spammers may be able  
18 to facially comply with the Act, including the opt-out  
19 provisions and notice of the fact that they're sending  
20 an advertisement, because they're using new technology  
21 to customize individual Emails or campaigns and thus  
22 avoid detection as a source of large volumes of spam.  
23 Some of this ties into zombies.

24 What, if any, are your thoughts about that and  
25 the impact it may have on the ultimate effectiveness of

1 CAN-SPAM?

2 Well, I've stumped the panel. I guess I get a  
3 prize for that one.

4 MS. FALLOWS: Okay, I'll add a comment. This is  
5 Deb.

6 MS. HARRINGTON-MCBRIDE: Thanks, Deb.

7 MS. FALLOWS: We're always surprised that there  
8 are a number of people who say they actually like  
9 getting spam, and it would stand to reason that if  
10 people felt that these were personalized messages that  
11 they would be more welcomed by more users.

12 There's also a very fluid sense of what actually  
13 is the definition of spam. Most everybody can agree on  
14 certain things like pornographic adult material is spam,  
15 but there's a softness in the definition of spam.

16 For example, many people will say that  
17 unsolicited mailings from public interest groups or from  
18 charities or from political groups is not spam. They  
19 are adhering to a more generous and open hearted  
20 definition of spam.

21 I would probably put this customized spam into a  
22 similar category. If people see that a message seems to  
23 be meant for them, or that they had more interest in the  
24 topic, then fewer people would be likely to say, "Hey,  
25 this is spam." They would say, "Oh, I'm not sure what

1 this is, but I don't mind this as much."

2 MS. HARRINGTON-MCBRIDE: Interesting. Anyone  
3 else have any thoughts to the extent to which spammers  
4 are using either new technology or adapting older  
5 technology methods to attempt to sort of fly beneath the  
6 radar in customizing their campaigns and making each  
7 Email appear to be unique?

8 MS. NEWITZ: This is Annalee with EFF. I guess  
9 to follow-up on what Deb is saying about sort of the  
10 soft definition of spam, if we're talking about people  
11 who are actually complying with CAN-SPAM using new  
12 technologies, then it's hard for me to understand how  
13 their mail is, in fact, going to be violating the Act  
14 and be spam, so maybe you could clarify that for me.

15 Is this mail that is in some way violating the  
16 Act or is it completely in compliance?

17 MS. HARRINGTON-MCBRIDE: Well, I think what the  
18 concern has been that I've seen expressed at least in  
19 the media is that CAN-SPAM may not be fully effective  
20 because indeed, those who want to send out lots of  
21 unsolicited commercial Email are in no way inhibited  
22 from doing so because they're able to do it. They can  
23 even appear to be compliant, but if each unique Email,  
24 for example, contains an opt-out but it's not really a  
25 valid opt-out, they appear facially to be in compliance,

1 but they may not actually be.

2 MS. NEWITZ: Right.

3 MS. HARRINGTON-MCBRIDE: And then filtering is  
4 less likely to be effective if each message is unique or  
5 seemingly unique.

6 MS. NEWITZ: Right, okay. I see what you're  
7 saying now. I would add that I think, yeah, that is an  
8 example of how there's always going to be a  
9 technological arms race here where if you try to pass a  
10 law or if you pass a law which is based on a level of  
11 technology, then you're always going to have a problem  
12 with new technologies defeating that law.

13 So clearly as another example, like a zombie  
14 machine that sends out authenticated spam, where  
15 technology is outrunning the law once again.

16 MS. HARRINGTON-MCBRIDE: Thank you, Annalee.  
17 Wrapping up this section, are there any other  
18 marketplace developments or technological changes that  
19 may affect the practicality or effectiveness of the Act  
20 that we haven't already talked about?

21 On to the next topic then, the second of the  
22 four that we'll address, and that is how to address  
23 commercial Email that originates in or is transmitted  
24 through or to facilities or computers in other nations.

25 This is another provision that Congress

1 specifically requested analysis on in our report, and so  
2 we're asking about this, and asking not only about the  
3 trends in transmission of Email through other countries,  
4 but also any initiatives or policy positions that the  
5 United States could pursue to increase the effectiveness  
6 of the Act.

7           So I guess my first specific question is: To  
8 what extent does commercial Email received in the U.S.  
9 originate in or get transmitted through other countries,  
10 and what are some sources of data on that that we should  
11 be considering?

12           MS. FALLOWS: This is Deb from the Internet  
13 Project. This is actually something I've been trying to  
14 follow myself, and I find it very difficult to sort  
15 through the reporting on this. I have seen figures that  
16 the U.S. is responsible for 60 percent of the spam.  
17 I've seen figures that they're responsible for  
18 15 percent of the spam, and most of it comes from China,  
19 Korea, Brazil, Spain.

20           It also seems to be a moving target, so I would  
21 just say that I don't know what I would recommend here.  
22 It's clear that it's all over the world, and we just had  
23 a lot of homework to do to try to figure out how to make  
24 this into a global effort.

25           With respect to one country that I know a little

1 bit about, which is China, I've been trying to follow  
2 Internet developments from China. It's very clear that  
3 the Chinese government is paying extremely strict  
4 attention to how the Internet is developing and wanting  
5 to strike a balance between having control over it for  
6 their own political purposes and also to encourage its  
7 use for its economic potential.

8 China has a distinct inclination to really grab  
9 for pornographic material on the Internet and suppress  
10 it entirely, and they're very effective at it. In that  
11 case, it that might be useful as an international global  
12 effort for us to cooperate with them on that.

13 My distinct sense is that what's really most  
14 important to the Chinese and a place where a lot of spam  
15 originates or flows through is their own domestic issue  
16 with the Internet, and secondarily would become  
17 international issues with the Internet, so I think  
18 you've got not only the kind of facts that you're  
19 dealing with and always in motion, but also the whole  
20 political fear that is going to be extremely hard to  
21 coordinate.

22 MS. HARRINGTON-MCBRIDE: Thank you. This is  
23 Katie. Something that Deb touched on there that was  
24 sort of a follow on question for me is: Are our methods  
25 for identifying the origin of the Email adequate? I've

1     seen some of the same disparate reports that Deb  
2     mentions about the source of spam and the volumes by  
3     country.

4             Does anyone on the call have any suggestions  
5     about methods for identifying the origin and the most  
6     effective ones that we have?

7             MR. EVERETT-CHURCH: This is Ray Everett-Church.  
8     I guess I would ask you to clarify the question a little  
9     bit in terms of trying to determine the origin. Are you  
10    looking for something beyond just being able to  
11    determine the source of a particular IP address and  
12    whether or not it may originate at a foreign location or  
13    intermediary server that you could trace to being a  
14    foreign source?

15            MS. HARRINGTON-MCBRIDE: Yes. I mean, I think  
16    that there are a handful of methods that I think are  
17    used in tracking back the originating point for spam, IP  
18    address being one, and presumably if all these studies  
19    show very different data, all the reports show different  
20    countries as the primary source of spam, it makes one  
21    wonder if everyone is drawing from the same pool of  
22    information or if there are multiple ways to get at  
23    where spam is originating, but it may be restating the  
24    obvious, but if anyone has anything that they would like  
25    to add, we want to be sure not to leave any stone

1 unturned.

2 MR. EVERETT-CHURCH: This is Ray Everett-Church  
3 again. I would say that to the best of my knowledge,  
4 still the predominant means of determining that sort of  
5 point of origin is indeed the tracing of the originating  
6 IP address. In most cases the spam that I receive that  
7 I'm able to determine an originating IP address, I can  
8 usually tell pretty quickly whether or not it's going to  
9 be a domestic or a foreign source.

10 In those cases, it's still exceedingly difficult  
11 to very convincingly forge IP addresses and avoid at  
12 least some level of being traced back to a point of  
13 origin. Now, what happens beyond this sort of top level  
14 Internet service provider information depends and varies  
15 quite widely.

16 So, for example, I might be able to determine  
17 that an IP address is traceable to a service provider in  
18 China, for example, but getting any information beyond  
19 that is extraordinarily difficult. In many cases those  
20 service providers are unresponsive. They may have laws  
21 or regulations or privacy policies that prohibit them  
22 from providing any additional information about who  
23 might be responsible for a particular Email message, and  
24 the ability of any sort of legal resource to cover that  
25 information is somewhat limited in that it can be

1 difficult to provide service or process of such to  
2 obtain through a court order or through a subpoena that  
3 sort of information.

4 MS. HARRINGTON-MCBRIDE: Thanks, Ray. Does  
5 anyone have any information, this is Katie again, on the  
6 amount of Email that originates in or is transmitted  
7 through other countries and whether this has changed  
8 since the passage of the Act?

9 I think I'll acknowledge that this goes back to  
10 what Deb and I have already said, which is that we're  
11 seeing reports that vary, and so it may be a difficult  
12 thing to judge since the baseline data maybe didn't all  
13 agree, but any suggestions on that?

14 I guess maybe to clarify, this is Katie again.  
15 In a former iteration of my work life, I worked on the  
16 Telemarketing Sales Rule, and there were widespread  
17 media reports at the time the Do Not Call Registry was  
18 developed that telemarketers in the United States would  
19 simply go offshore so that they could avoid complying,  
20 and at the same time, when CAN-SPAM was passed, I think  
21 there were some similar reports that suggested that to  
22 the extent that Emailers in the U.S. were concerned  
23 about the Act and its implications for their business  
24 model, they might simply go offshore.

25 So any data does show the volume of Email

1     originating in various countries at the time of the Act  
2     passage and what it is now would be helpful, and that's  
3     what we're trying to sort of get at there.

4             MR. EVERETT-CHURCH: This is Ray Everett-Church.  
5     I'm unaware of particular studies on this point. I'll  
6     say anecdotally I'm not aware of any increased exodus of  
7     offshore on the part of spammers.

8             Just in my surveys of the spam marketplace, it  
9     seems to me that most of those spammers who have the  
10    wherewithal to take their operations offshore did so  
11    over the course of several years and did not necessarily  
12    make that jump in direct response to the CAN-SPAM Act.

13            MS. HARRINGTON-MCBRIDE: Okay. Thank you.

14            MR. HOOFNAGLE: This is Chris from EPIC. I  
15    think your question illustrates one of the problems that  
16    Annalee identified earlier, and that is that CAN-SPAM  
17    doesn't focus a lot on the technology of sending Email.

18            MS. HARRINGTON-MCBRIDE: Chris, I'm sorry, your  
19    dropping out about every second syllable. Are you close  
20    enough to your phone, do you think?

21            MR. HOOFNAGLE: Yes, can you hear me now?

22            MS. HARRINGTON-MCBRIDE: Yes, that sounds  
23    better. We'll stop you though if it becomes difficult  
24    to understand. We just want to be sure we get  
25    everything that you're saying down. Thanks.

1           MR. HOOFNAGLE: This is Chris from EPIC, and to  
2 amplify something that Annalee said earlier, and I think  
3 it marginally responds to this question. CAN-SPAM  
4 really is focused on a certain method of marketing, and  
5 I think that we've overlooked some other tools that you  
6 can normally use in consumer protection to address  
7 illegal activities, whether they're on shore or off.

8           One of those is advertiser liability. If a  
9 spammer moves offshore, I think you'll find that most of  
10 the time they are advertising a product from a company  
11 that can be bought in America or from an American  
12 company.

13           So I did want, at some point in this call, to  
14 emphasize that instead of focusing on the specific  
15 technology, it might make sense to start pinning some  
16 liability to advertisers when they hire a spammer or  
17 when they're put on notice that an independent was  
18 engaged in an illegal form of marketing.

19           MS. HARRINGTON-MCBRIDE: Thanks, Chris. This is  
20 Katie from the FTC. I began this part of the  
21 questioning without noting that, of course, both in the  
22 TSR context and the CAN-SPAM context, the FTC's response  
23 to these suggestions that going offshore somehow  
24 provides protection is to note that we have a fairly  
25 robust law enforcement history of going after folks who

1 operate from beyond the U.S. boundary, but do in fact  
2 market to U.S. consumers.

3 And some of our CAN-SPAM enforcement work has  
4 done just as Chris suggested, which is to address  
5 advertiser liability, and even to go after those in  
6 other nations, sometimes with the assistance of law  
7 enforcement agencies in other countries.

8 So it's not necessarily the case that they will  
9 be protected. It has, in fact, been proven that the FTC  
10 will go after them. I think it's more a misconception,  
11 and there were these earlier reports, and I thought we  
12 should track to see if anyone knew of any data that  
13 suggested that folks were acting to those reports.

14 Another point on the internal front, and this  
15 is Katie still, as many of you now, the FTC does work  
16 closely with various international organizations to  
17 monitor Email trends around the world and laws and other  
18 initiatives, and I wonder if anyone has any comments on  
19 the initiatives.

20 I don't have someone here with us from our  
21 international division, but some of these initiatives  
22 include working with the OECD and working on an  
23 initiative called the London Action Plan to work  
24 cooperatively with law enforcement agencies around the  
25 world, to more effectively trace spam, to provide access

1 to data and to enable law enforcement agents to work  
2 more effectively together to find those who are abusing  
3 Email.

4 I'm wondering if anyone has any thoughts about  
5 the initiatives that have been taken or others that  
6 could be undertaken to try to improve the effectiveness  
7 of the Act.

8 One other thought, it's been suggested that  
9 particularly in the international arena, it would be  
10 useful to have stricter standards for domain name  
11 registrars to require that truthful information be given  
12 them, and thus be available to law enforcement agencies.  
13 To what extent would these stricter standards, if they  
14 could be implemented, help to address the spam problem?

15 MR. HOOFNAGLE: This is Chris Hoofnagle from  
16 EPIC. We are in strong opposition to requiring  
17 truthfulness in domain registrations. There are a  
18 number of reasons for this.

19 One is because it can inhibit First Amendment  
20 protected anonymous speech, which of course here in  
21 America is protected but is not necessarily protected in  
22 other countries where anonymity would be even more  
23 important.

24 Where truthfulness in who is registering is  
25 required, the bad guys will still circumvent the

1 requirements by registering under a corporate name or  
2 using a corporate registrar whereas the average person  
3 will comply with the law and end up having to identify  
4 themselves.

5 Finally, there are significant problems with the  
6 Who Is database. It is not privacy friendly, in that it  
7 requires individuals to divulge personal information but  
8 does not place any limit on the use of that personal  
9 information.

10 So it really is an example of a system where a  
11 government or a business is encouraging you to disclose  
12 personal information, and then that information is  
13 simply provided to the world for anyone to use for any  
14 purpose.

15 So, for instance, it's not just a matter of  
16 protecting anonymous speech. It's a matter of  
17 protecting one's self from unwanted petitions, because  
18 if you put in truthful information, you'll very quickly  
19 begin to receive deceptive mailings from other  
20 registrars trying to get you to change your hosting or  
21 your registrar company.

22 MS. HARRINGTON-MCBRIDE: Thank you.

23 MR. EVERETT-CHURCH: This is Ray Everett-Church.  
24 Let me echo Chris's points. While I think it would be  
25 helpful in some instances to have more truthful

1 information in a domain name record, the true bad actors  
2 out there have many methods by which to avoid being held  
3 accountable, at least through a domain name registration  
4 system, so there are any number of ways of putting  
5 information that may be truthful, yet be completely  
6 uninformative, regarding who should be held responsible  
7 for a particular mailing.

8           So in this case a requirement of truthful domain  
9 name registration information doesn't necessarily  
10 advance the cause of fighting spam, and let me also say  
11 that it's also an instance where some sort of  
12 differentiation between commercial usage and non  
13 commercial usage might be appropriate where in many  
14 cases we've advocated -- folks have advocated for  
15 particular restrictions on commercial applications or  
16 commercial usage of domains or of particular Internet  
17 connections and been able to separate those from say  
18 requirements that would apply to an individual.

19           Making that differentiation helps to avoid the  
20 sorts of concerns that Chris has raised in terms of any  
21 backlash against an individual who might be seeking to  
22 exercise legitimate free speech rights while avoiding  
23 any retribution from an oppressive government or an  
24 oppressive employer or whoever it may be.

25           MS. HARRINGTON-MCBRIDE: Thank you.

1           I would like to move on to our third point here,  
2           but I want to note here, we're going to try to stick to  
3           the two-hour limit, but I'll mention at the end of the  
4           call, if you have additional information that occurs to  
5           you after we hang up and you would like to provide it,  
6           you're certainly welcome to send me an Email, so I don't  
7           want to cut this off prematurely, but I do want to be  
8           sure to cover the specific provisions of the Act.

9           The third issue, just before we get to those  
10          provisions, relates to protecting consumers, including  
11          children, from receipt and viewing of commercial Email  
12          that is obscene or pornographic.

13          Of course the first question here is: How  
14          effective has the FTC's sexually explicitly labeling  
15          rule, which was promulgated by the FTC pursuant to the  
16          CAN-SPAM Act -- how effective has that been in  
17          protecting consumers, including children, from receiving  
18          and viewing obscene or pornographic Email?

19          MS. FALLOWS: This is Deb from the Pew Project.  
20          We actually have some before and after figures on the  
21          amount of pornographic spam that people report that  
22          they're receiving. I can send you those exact numbers,  
23          but there was a distinct drop in people reporting that  
24          they're getting pornographic spam after the CAN-SPAM Act  
25          has been in effect awhile.

1 MS. HARRINGTON-MCBRIDE: I think that is  
2 something echoed by the recent spam index that showed  
3 that I think now their focus is -- this is Clearswift's  
4 spam index which was reported about a week ago I guess  
5 that pornographic spam now accounts for 5 percent of all  
6 Email that they're assessing, and that's four times less  
7 than in June 2003.

8 MS. FALLOWS: This is Deb again. So I certainly  
9 wouldn't take issue with any of that, but what I would  
10 say is that for the people who receive porn spam it's  
11 extremely horrible. We had a marked response with  
12 respect to pornographic spam. It was the most troubling  
13 of any kind of spam that people received. To this day I  
14 get Emails -- this is anecdotal now -- but to this day I  
15 get Emails from parents who are writing to say, "Oh, I  
16 have seen your study, but please, what can you do to  
17 help me, there's nothing that I can do about this porn  
18 spam that I continue to receive."

19 I can either read to you or forward to you in an  
20 Email the most recent one I have, which goes into the  
21 poignant category of real life stories of parents who  
22 are getting the porn spam.

23 MS. HARRINGTON-MCBRIDE: I would appreciate it  
24 if you would forward it, Deb.

25 MS. FALLOWS: Sure.

1 MS. HARRINGTON-MCBRIDE: That would be great.  
2 In addition to the rule that the FTC promulgated  
3 pursuant to the CAN-SPAM Act, obviously private sector  
4 tools such as those made available by ISPs and Email  
5 service providers and by private software companies  
6 exists to shield consumers from obscene or pornographic  
7 Email.

8 Any thoughts about how effective this kind of  
9 software is?

10 MS. FALLOWS: This is Deb from the Pew Project.  
11 One thing that I've been surprised to see in a lot of  
12 our data is how many people say that they still feel  
13 they can't control the automatic viewing of the content  
14 of their message; in other words, when they open their  
15 inbox, they don't just see the list of messages, but  
16 they see at least a partial viewing of the content of  
17 each, or the text, or the photo, the image or whatever  
18 it is of each individual message.

19 MS. HARRINGTON-MCBRIDE: In a preview page or  
20 something like that?

21 MS. FALLOWS: Yes, yes, and that's been  
22 something that's particularly troubling to people. I  
23 don't know myself, but I've heard different discussions  
24 about how you're either able or not able to turn off  
25 that feature, and enough people have told me that in

1 certain circumstances you cannot turn it off, that that  
2 feature alone would be something that is certainly worth  
3 making possible.

4 The other suggestion that I've heard is that the  
5 law be written in some way to say that the body of the  
6 message cannot contain any of the actual pornographic  
7 texts or images, but that it only contains links to lead  
8 to that content.

9 MS. HARRINGTON-MCBRIDE: Okay. That's sort of  
10 the Brown Paper Wrapper effect of our rule.

11 MS. FALLOWS: Okay.

12 MS. HARRINGTON-MCBRIDE: I don't know whether  
13 you're suggesting further efforts to ensure that that be  
14 complied with.

15 MS. FALLOWS: I don't know specifically about  
16 the Brown Paper Wrapper, and I didn't know that that  
17 particular item was something that was already on the  
18 table. I should have guessed that you had thought of  
19 it.

20 MS. HARRINGTON-MCBRIDE: Actually with the  
21 urging of Congress, we incorporated into our sexually  
22 explicit labeling rule a provision not only that the  
23 sexually explicit Emails be labeled, that is so that  
24 there would be some way to identify it if you aren't  
25 looking at a preview page, so you can make a decision

1 based on that subject line tag, but also that when the  
2 initially viewable area should not contain any imagery,  
3 and in fact that folks should be protected from viewing  
4 that unless they make sort of an affirmative choice to  
5 either scroll down or click on a link.

6 This is Katie again. There are several kinds of  
7 protections it seems to me from doing some very basic  
8 research that ISPs offer having to do with protecting  
9 children in particular, but all users can benefit I  
10 think from this.

11 Some include software that would disable a link  
12 in Email if it's sent by someone who is not in a  
13 subscriber's address book, technologies that don't allow  
14 the instantaneous receipt of Email from anyone but folks  
15 that a subscriber has agreed to receive Email from.

16 Are these approaches in anyone's estimation  
17 useful or are there more approaches out there that we  
18 should be looking at?

19 MS. NEWITZ: This is Annalee with EFF. I can't  
20 address those particular approaches by the ISPs, but I  
21 wanted to bring up another kind of way that spam for  
22 children, porn spam for children is attempting to be  
23 regulated, and that's through laws that have been  
24 proposed and passed in a couple of states, Utah and  
25 Michigan and some others that have to do with creating

1 lists of children, known children's Email addresses.

2 MS. HARRINGTON-MCBRIDE: Yes.

3 MS. NEWITZ: We're very concerned about this  
4 because that obviously can lead to tremendous privacy  
5 violations since there's going to be some agencies, a  
6 state agency that's keeping this list, and the idea is  
7 that commercial entities that want to comply with the  
8 law and send commercial mail but not send it to children  
9 will have to check their list against these lists to  
10 find out if there's any children on their list.

11 It's not just for porn. It's also for gambling  
12 and any kind of item that is not appropriate for  
13 children to be consuming, and it's our theory that, in  
14 fact, CAN-SPAM may actually preempt these state laws,  
15 which would actually be a nice outcome for privacy  
16 advocates in particular, since as I said, I think these  
17 lists of children's names are extremely vulnerable, and  
18 it would be very easy for someone to use various tricks  
19 or scams to find out the legitimate Email addresses of  
20 children and access those children while pretending to  
21 be checking their commercial list against that list.

22 So that's something interesting that's come up,  
23 and I think we're going to see more and more states  
24 trying to come up with laws like that that I think will  
25 end up leaving children more vulnerable rather than less

1 vulnerable.

2 MS. HARRINGTON-MCBRIDE: Yes, and I'm sure  
3 you're aware of our Do Not Email Registry Report and the  
4 justification in part for not, last summer, implementing  
5 a Do Not Email Registry. One of the ideas is that again  
6 the data can't always be safeguarded and that  
7 particularly with regard to children's Email addresses,  
8 if they were identified in a subset as such, that there  
9 could be real concerns, so that is legislation that we  
10 continue to watch with interest as well.

11 MS. FALLOWS: This is Deb again. Katie, back to  
12 your point about disabling links or blocking from  
13 certain senders and so forth.

14 MS. HARRINGTON-MCBRIDE: Yes.

15 MS. FALLOWS: I would just reiterate again that  
16 anything that requires this kind of individualized  
17 effort from users is something that you will find very  
18 few users actually taking advantage of. It's too  
19 clumsy, and it's too time consuming, and it's too  
20 demanding.

21 With problems like adult content on the  
22 Internet, we find that most people or most parents will  
23 institute a combination of things that are much more  
24 kind of normal. They'll have house rules about what  
25 their kids are allowed to see. They'll block certain

1 basic web sites. They'll monitor their kids by kind of  
2 checking back on what they've been looking at. They'll  
3 keep computers in public spaces where they can look over  
4 their shoulders.

5 These kinds of home grown methods are what  
6 people are doing rather than the finely tuned methods of  
7 trying to keep control.

8 MS. HARRINGTON-MCBRIDE: Thank you. I guess  
9 that sort of brings me to a question that I think you've  
10 started to answer, Deb, which is: Are there other  
11 options that consumers are availing themselves of, and  
12 are there any statistics about those, for example, spam  
13 filtering or blocking software that consumers are  
14 installing specifically to deal with concerns about  
15 receipt of pornographic Email?

16 It's more I think a question about data out  
17 there that would suggest in what quantities this, Deb  
18 things are being scooped up.

19 MS. FALLOWS: This is Deb. We have data on  
20 Internet use in general, but not specifically on Email  
21 blocking and use.

22 MS. HARRINGTON-MCBRIDE: Okay.

23 MS. FALLOWS: And I actually don't know about  
24 what Email data.

25 MS. HARRINGTON-MCBRIDE: Anyone else have any

1 suggestions for sources of data about the extent to  
2 which consumers are investing in additional blocking  
3 technologies?

4 MS. FALLOWS: Katie, this is Deb. I would just  
5 go straight to AOL and Yahoo and Hotmail and all the big  
6 ISPs. I would think they would have that.

7 MS. HARRINGTON-MCBRIDE: They've certainly been  
8 very helpful to us in the past 18 months.

9 MS. FALLOWS: This is Deb still. Just as one  
10 interesting real life data point here: Parents and kids  
11 are very consistent about saying that they all know kids  
12 are doing things on the Internet that parents don't want  
13 them to do. Two-thirds of parents and of kids say that  
14 they believe kids do things online that they wouldn't  
15 want their parents to know about. So as much as  
16 whatever kind of vigilance and oversight is going on,  
17 it's only effective as the security of the cookie jar  
18 lid.

19 MS. HARRINGTON-MCBRIDE: I'm hugely relieved  
20 that I'm here today in my capacity as an FTC lawyer and  
21 not a mom, because that would be troubling if I were  
22 thinking in terms of my own kids.

23 Our fourth topic, and the one that we'll spend  
24 pretty much the next 29 minutes covering, is the  
25 effectiveness of the various provisions of the Act. I

1 presume that most of you are pretty familiar with the  
2 Act, but what I've done is really just created a laundry  
3 list here of its various provisions in general, and you  
4 may not have something to say about many of the 15 or so  
5 that we'll talk about, but you may have a lot of data on  
6 one.

7 I'll just go through them serratum, and you  
8 should feel free to tell us what your thoughts are about  
9 how effective this, Deb provisions have been and whether  
10 there are any concerns about enforcement of them.

11 We'll begin, again we're kind of going page by  
12 page through the act, with the criminal provisions that  
13 empowers the Department of Justice to use its authority  
14 to go after those who violate the provisions of the Act  
15 rising to the level of making something a criminal  
16 violation for sending spam, so we'll talk about the  
17 criminal provisions and the penalties under the Act,  
18 whether those are sufficient as a deterrent and any data  
19 that you might have on that.

20 It doesn't sound like there's too much feedback  
21 on the criminal provisions.

22 There are far more individualized civil  
23 provisions, so we'll take those one by one, the first  
24 being the prohibition in the Act on inclusion of false  
25 header information. This provision applies to both

1 commercial Email messages and transactional or  
2 relationship messages. It's the provision in the Act  
3 that does apply to both. Most of the provisions as you  
4 know only apply to commercial Email.

5 Has this prohibition on false header information  
6 been an effective one, and do you have any thoughts  
7 about its enforcement?

8 MR. EVERETT-CHURCH: This is Ray Everett-Church.  
9 I don't have any specific examples to cite, but my  
10 understanding is that there remain a good number of  
11 products on the market for automating the forgery of  
12 headers in various sort of spam software tools, and I'm  
13 not aware of any enforcement efforts that have targeted  
14 software or services that specifically enable those  
15 sorts of violations, but that would be one area in which  
16 I think there might be some room for additional  
17 enforcement.

18 MS. HARRINGTON-MCBRIDE: Thank you.

19 MS. NEWITZ: This is Annalee Newitz from EFF.  
20 Our concern again with activist groups and charities and  
21 such has been that often this, Deb groups find that  
22 their efforts to do organizing or fund raising are  
23 somewhat inhibited because they're just not really sure  
24 how to have an accurate subject line, and whether they  
25 would fall into the status of commercial mail or not.

1           So I think that one of the difficulties in  
2 enforcement is that it's causing a certain amount of  
3 silencing of groups that would normally feel comfortable  
4 sending out mass Emails.

5           MS. HARRINGTON-MCBRIDE: Since my Email address  
6 is all over the web, I'll say to you not so much for the  
7 purposes of this transcript, but in general that if you  
8 have folks you hear from who have concerns about  
9 compliance, you should feel free to refer them to the  
10 staff attorneys who work on this. I am one of them, and  
11 I can provide you my phone number in a call after this,  
12 because we do get a lot of traffic on this and other  
13 rules that the FTC enforces where folks are just asking  
14 questions, you know, I'm a small organization and how do  
15 I go about complying.

16           We do our level best to make sure that they have  
17 the tools to go out there and continue to conduct  
18 business, so to the extent we're able to help, we're  
19 glad to.

20           MS. FALLOWS: Okay, great. Thanks.

21           MS. HARRINGTON-MCBRIDE: Sure.

22           So the provisions on false header information  
23 and deceptive subject lines, any further thoughts?

24           One of the primary consumer protections  
25 contained in the CAN-SPAM Act, of course, is the

1 requirement that commercial Emails include a functioning  
2 returning address or other opt-out mechanism that must  
3 work for 30 days beyond the sending of the Email, and  
4 this provision also includes a safe harbor where the  
5 mechanism is temporarily and unexpectedly unavailable.  
6 Any thoughts about that provision and its efficacy and  
7 the enforcement of it?

8 A related provision is the prohibition on  
9 transmission of commercial Email after someone has opted  
10 out, a recipient has opted out, and currently senders  
11 have ten days to comply with this, Deb requests. This  
12 is a provision that is currently under review in an  
13 extant rulemaking that the FTC is conducting. We've  
14 called it the discretionary rulemaking.

15 Any thoughts about the provision that prohibits  
16 transmission of commercial Email after an opt-out or the  
17 ten-day allowable period?

18 MR. HOOFNAGLE: Yes, this is Chris Hoofnagle  
19 from EPIC. We have commented that the ten-day period is  
20 probably too long, and that there are tools available in  
21 many contexts to handle opt-outs immediately.

22 Now, we understand that companies have different  
23 complexities in their marketing campaigns, but if sales  
24 and purchases can be negotiated in a matter of minutes,  
25 there really is no reason why opt-outs should not be

1 able to be handled in a similar fashion.

2 MS. HARRINGTON-MCBRIDE: Thanks, Chris.

3 MR. HOOFNAGLE: Sure.

4 MS. FALLOWS: Katie, this is Deb. This is a  
5 general comment on doing something like opting out of  
6 future Emails. It seems that the general public is  
7 being trained somewhat to not click on links or not  
8 provide information requested in unsolicited Emails. So  
9 in a way, this is kind of self-defeating behavior  
10 because people are also reluctant to click to opt-out  
11 because they don't trust that it's going to be used for  
12 that purpose.

13 So the good behavior that people have learned  
14 about not clicking on anything in unsolicited Emails is  
15 thereby causing the problem for opt-outs as part of the  
16 spam solution.

17 MS. HARRINGTON-MCBRIDE: You know, this is  
18 Katie, and that leads me, Deb, to two follow-up  
19 questions. One, is there any data, whether it's  
20 generated by Pew or another source, on the willingness  
21 of recipients to click on opt-out links and the rate at  
22 which they do it, and certainly any longitudinal data  
23 that suggests it was a different number in December  
24 of 2003 than it is today would be helpful, and secondly,  
25 there are certainly reports in the popular press about

1 the possibility of downloading malware on to a  
2 recipient's computer if indeed the opt-out link is  
3 clicked on?

4 So far what we've seen is mostly anecdotal, but  
5 if anyone has any further data on that issue, that is  
6 one that we're very interested in.

7 MS. FALLOWS: Katie, I don't have that, this is  
8 Deb, but I can look around and see if somebody does, if  
9 you want us to try to find that.

10 MS. HARRINGTON-MCBRIDE: That's very helpful or  
11 we're happy to follow on any leads if you have  
12 individuals you think we ought to talk to. We would be  
13 happy to do that.

14 MS. FALLOWS: Okay, I will ask. I will ask  
15 around and give that to you.

16 MS. HARRINGTON-MCBRIDE: Thank you.

17 MR. HOOFNAGLE: This is Chris from EPIC. We are  
18 one of the groups that tells consumers not to click on  
19 opt-out links from spam, and the reason why we continue  
20 to do that is that CAN-SPAM does not include a private  
21 right of action for individuals, and until it does,  
22 there isn't a strong enough guarantee for accountability  
23 in compliance with the law that would give us enough  
24 comfort to tell consumers to click on the opt-out links.

25 MS. HARRINGTON-MCBRIDE: Okay. Are you aware of

1 anything, Chris -- we've seen some media reports that  
2 there can be or there's at least the potential for  
3 downloading malware by clicking on this. Are there any  
4 sort of real life stories that anybody has to tell about  
5 that?

6 MR. HOOFNAGLE: This is from Chris from EPIC.  
7 We have no evidence of that practice, although it's  
8 obviously possible to spread Spyware in that way. This  
9 is one issue where we suffer from some observation error  
10 simply because consumers often cannot identify where  
11 malware originated, and it might be from a drive-by  
12 download or it might be from the link they have clicked  
13 on or software that their children have installed, so  
14 it's an issue that probably would require the Commission  
15 to actually go through expanded database and click on  
16 some of those opt-out links.

17 MS. HARRINGTON-MCBRIDE: Okay. Thank you. The  
18 next provision is the requirement that commercial Email  
19 include an identifier, that is, a notice to the  
20 recipient that the message is an advertisement or  
21 solicitation. Any thoughts about that provision and its  
22 effectiveness and enforcement?

23 There are two companion requirements, the next  
24 being the commercial Email include a clear and  
25 conspicuous notice of the recipient's right to opt-out

1 of receiving future Email. That's tied in, of course,  
2 to the opt-out provisions, but there needs to be notice  
3 in the Act. Any thoughts about the effectiveness of  
4 that provision or its enforceability?

5 The third of that disclosure requirement is of  
6 course that commercial Email must include the valid  
7 physical postal address of the sender. That's also a  
8 provision for which the FTC has exercised its  
9 discretionary rulemaking authority and gone out with an  
10 interpretation that a valid -- that either a commercial  
11 mail drop or Post Office Box would suffice as a valid  
12 physical postal address.

13 Are there any thoughts about the inclusion of  
14 this requirement, the disclosure, the rulemaking or the  
15 enforcement of that provision?

16 MR. HOOFNAGLE: This is Chris from EPIC.  
17 Allowing a business to identify itself by a PO Box  
18 creates hurdles in litigation, especially for  
19 unsophisticated or pro se litigators. It would be more  
20 consumer friendly to have a requirement that an actual  
21 full address be specified.

22 MS. HARRINGTON-MCBRIDE: Thank you. The  
23 CAN-SPAM Act contains provisions that allow for  
24 enforcement of the Act by the FTC, other federal  
25 agencies, the Attorneys General, and Internet access

1 services, and each of this, Deb groups has specific  
2 penalties that it can obtain for violations.

3 Any thoughts about the penalties or the Act's  
4 inclusion of certain practices as aggravated violations  
5 which can lead to treble damages if a primary provision  
6 of the Act's is violated, and one of this, Deb practices  
7 has been engaged in? This, Deb include harvesting of  
8 Email addresses or dictionary attacks and some others?

9 We're down to just four more provisions. The  
10 next is the sexually explicit label requirement that's  
11 included in the Act, and the Act directed the FTC to  
12 promulgate rule which was done last April. Any thoughts  
13 about the Act or the rule?

14 MS. FALLOWS: Katie, this is Deb. I would just  
15 say again that based on all the surveys that we've done,  
16 this is the single item that is most troubling to users,  
17 and speaking as their proxy, I would say that users  
18 would want this above and beyond anything else.

19 MS. HARRINGTON-MCBRIDE: Thank you.

20 The Act also includes a provision which is  
21 available for FTC enforcement only, which prohibits  
22 promotion of a person's trade or business in a  
23 commercial Email message, the transmission of which  
24 violates Section 5(a)(1) of the Act, which is the false  
25 or misleading header information provision. Any

1 thoughts about that provision?

2 Another provision of the CAN-SPAM Act preempts  
3 state law, except those that are not specific to Email  
4 or which address the fraudulent nature of Email. Any  
5 thoughts about the preemption provisions of the Act?

6 MR. HOOFNAGLE: This is Chris from EPIC. EPIC  
7 and perhaps most consumer groups are strongly opposed to  
8 preemption of state law on consumer protection for many  
9 reasons that are documented in detail on our web site,  
10 but most notably, because the states have been faster to  
11 react to new consumer protection problems than the  
12 federal government has.

13 MR. EVERETT-CHURCH: This is Ray Everett-Church.  
14 I just echo Chris's point that I think the preemption  
15 provision of the CAN-SPAM Act has been just as effective  
16 as it was intended to be in forestalling and taking the  
17 wind out of the sails of any efforts by states to  
18 respond to changes in spam tactics and practices.

19 The preemption remains an area of great concern  
20 for those who have been looking to the states to  
21 continue to push the enforcement efforts and experiment  
22 with new approaches that might be more effective than  
23 CAN-SPAM has been thus far.

24 MS. HARRINGTON-MCBRIDE: Thanks, Ray.

25 MR. HOOFNAGLE: This is Chris again from EPIC.

1 If I may make one further point.

2 MS. HARRINGTON-MCBRIDE: Certainly.

3 MR. HOOFNAGLE: Many in the Email marketing  
4 industry say that they don't want to comply with the  
5 patch work of state laws, this argument should be viewed  
6 with a lot of skepticism by the Commission because there  
7 are compliance tools that are advertised on the various  
8 partner web sites, so at the same time that they are  
9 telling Congress that they can't comply with state laws,  
10 they're actually advertising compliance tools to do so.  
11 Furthermore the companies have very sophisticated  
12 profiling systems, that can in fact profile people down  
13 to the ZIP+4 level, and if these companies can treat  
14 people differently in the ZIP+4 level, they should be  
15 able to use the same technology to deal with different  
16 state laws

17 MS. HARRINGTON-MCBRIDE: Thanks, Chris.

18 The final provision that I wanted to ask about  
19 is the provision that addresses wireless messages and  
20 gives the FCC, the Federal Communications Commission,  
21 authority to regulate that. Their rulemaking is  
22 complete on this topic, and I wonder if anyone has any  
23 thoughts about the inclusion in the Act of this  
24 provision or the FCC's rule?

25 Okay. Well, I very much appreciate all of you

1 taking time to talk with us and to share your knowledge  
2 with us. As I mentioned, and as I think most of you  
3 know because you've been involved in other studies  
4 pursuant to the CAN-SPAM Act that the FTC has done, it's  
5 very important for to us have this dialogue to be able  
6 to best report to Congress on the effectiveness and  
7 enforcement of the Act, and we really appreciate your  
8 taking the time today to talk with us.

9 If there are any other data sources, whether  
10 they be individuals or studies or articles, that you  
11 think that we should review or if you have any further  
12 thoughts on the issues that we've talked about today,  
13 please feel free to contact any of us by Email. I'll  
14 give you my Email address, which is cmbride@ftc.gov.  
15 That's C M C B R I D E @ F T C . G O V . We would be more  
16 than happy to hear from you.

17 We are on a fairly short time frame here, so to  
18 be able to hear from you within the last three weeks or  
19 so would be very advantageous. Obviously if you come  
20 upon data after that and would like to transmit it, we  
21 will do our level best to make sure that we take account  
22 of that in production of this report.

23 And on a housekeeping note, I want to let you  
24 know that once the transcript from today's call is  
25 available, it will be circulated to all participants so

1 that you may have an opportunity to review and correct.  
2 Because there are so many participants on our various  
3 calls, this is one of the smaller ones, which could be  
4 why we high-jacked you, Deb, and made you into a privacy  
5 professional, we want to be sure that if you do make any  
6 corrections, if you could send them to us in red line  
7 format, it will really expedite our ability to process  
8 through those changes and finalize the transcript.

9 We'll be asking for fairly quick turnaround on  
10 this. Allyson Himelfarb is the contact person, and  
11 she'll be in touch with you all as soon as the  
12 transcripts are ready, and you can communicate your  
13 thoughts on the transcript back to her.

14 Again, thank you so much for taking time, and  
15 please feel free to keep the channels open on this  
16 report. Again, Annalee, on any of the compliance  
17 concerns that your constituents may be having, we'll be  
18 glad to talk to them.

19 MS. NEWITZ: Thank you. I'm sorry. Can you  
20 spell your Email address one more time? I know you  
21 already did it like six times.

22 MS. HARRINGTON-MCBRIDE: No problem. It's C M C  
23 B R I D E @ F T C . G O V like Catherine McBride, C.  
24 McBride.

25 Well, thank you all very much. We'll look

1 forward to touching base with you in the future.

2 (Whereupon, at 2:55 p.m. the meeting was  
3 concluded.)

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

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

CERTIFICATE OF REPORTER

DOCKET/FILE NUMBER: P044405  
CASE TITLE: REPORT TO CONGRESS  
HEARING DATE: JULY 20, 2005

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the steno notes transcribed by me on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED: SEPTEMBER 16, 2005

\_\_\_\_\_  
DEBRA L. MAHEUX

CERTIFICATION OF PROOFREADER

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

\_\_\_\_\_  
DIANE QUADE