

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

Do Not E-Mail Registry
Meeting

Wednesday, March 10, 2004
10:00 a.m.

Federal Trade Commission
6th and Pennsylvania Avenue, N.W.
Room 432
Washington, D.C.

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

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

PARTICIPANTS:

From the Commission:

Dan Salsburg

Colleen Robbins

Sheryl Drexler

Kim Lucas

Morning Session:

Elizabeth Treanor, National Retail Federation

Scott Silverman, Shop.org

Scott Richards, MBNA

Beth Marshall, MBNA

John Collingwood, MBNA

Steve Richter, E-Mail Marketing Association

P R O C E E D I N G S

1
2 MR. SALSBURG: We are here with a court
3 reporter, so we're going to do a few formalities before
4 we start.

5 Today is Wednesday, March 10, 2004. It's about
6 10:00 in the morning, Eastern Time. We are meeting with
7 Elizabeth Treanor from the National Retail Federation;
8 Scott Silverman of Shop.org; Scott Richards, Beth
9 Marshall, and John Collingwood from MBNA; and joining us
10 on the phone, is Steve Richter from the E-mail Marketing
11 Association.

12 The purpose of this meeting is to discuss a
13 possible National Do Not E-mail Registry. We're having a
14 court reporter transcribe this meeting because we are
15 intending to cite it in a report to Congress that we're
16 required to complete by June 16th, pursuant to Section 9
17 of the CAN-SPAM Act.

18 As you all know, Section 9 of the CAN-SPAM Act
19 directs the FTC to submit to Congress a report detailing
20 a plan and a timetable for implementing a National Do Not
21 E-mail Registry. The report is supposed to list any
22 concerns that we have regarding security, privacy,
23 enforceability, or other issues.

24 So we've been meeting with a host of people who
25 we know have an interest in spam in general, and also in

1 Do Not E-mail. We have been transcribing all of these
2 conversations, where possible. We appreciate your coming
3 in to talk with us.

4 We thought that the best way to proceed would
5 be to throw out some possible models for Do Not E-mail
6 Registries, and hear your thoughts, based on the
7 backgrounds that you come from and the types of firms
8 that you represent.

9 The first model is one that's probably familiar
10 to most of us; and that's the National Do Not Call
11 Registry Model. Under this model, a consumer would
12 register his or her e-mail address with a central
13 registry, presumably at the FTC.

14 This database of registered e-mail addresses
15 could either be made directly available to marketers, who
16 could then scrub their lists against this Registry and
17 refrain from sending unsolicited commercial e-mail to
18 people whose addresses were listed on the Registry. Or,
19 conceivably, the FTC itself, or some third party, could
20 do the scrubbing, and then send back a cleaned list of e-
21 mail addresses that weren't on the Registry.

22 Do you have any thoughts on that sort of
23 Registry model?

24 MS. MARSHALL: I think, on the plus side,
25 there's ease in registration for consumers. There are

1 some concerns that I would have for the people that would
2 have to access that list. One would be -- in the Do Not
3 Call model, marketers purchase a copy of the list or
4 download a copy of the list.

5 My concerns would be the security of that
6 information, once it's disseminated, if you will; how
7 people that access it are certified as using it for the
8 right reasons.

9 If, alternatively, that list was in a central
10 place and your marketing list would be sent there to be
11 scrubbed, what type of bottleneck would that create for
12 commerce; where you've got many marketers attempting the
13 same function? Is it in one place? Is it in a limited
14 number of secure places where there's a mirror image of
15 that list? Practical concerns on, how do you scrub --
16 how do you do it?

17 MR. RICHARDS: I think, on either one, the
18 authentication mechanism, whether it be to the central
19 model or to the distributed, is a concern.

20 MR. SALSBURG: What do you mean by "the
21 authentication"?

22 MR. RICHARDS: Candidly, if I was a bad guy,
23 one of my deals would be to go through the process and
24 develop myself as a "certified", for lack of a better
25 term, marketer; come in looking -- whether it's at the

1 distributed point or at the central database --
2 completely legitimate; and then, basically, scrub; and
3 have access to the data.

4 I guess the other concern with the central
5 model or the distributed model is the security concern.
6 One, once the data is out, it's out. It takes one time
7 for the bad guys to get it, and the database itself
8 really doesn't have value.

9 Second, if I'm a bad guy and I get in, do I
10 want to corrupt the data? Do I want to make the database
11 unworkable in some form or fashion, just because I'm a
12 hacker and I like to do those things; the challenge that
13 it presents?

14 MR. SALSBURG: Would the database have value to
15 a spammer?

16 MR. RICHARDS: Absolutely. You have created --
17 versus a bunch of smaller databases out there where they
18 go to Company X, Y, or Z, you've created one nice, neat
19 place for them to go to to get 300 million -- I think
20 that's the number in the example of e-mail addresses.

21 MR. SILVERMAN: And it would be real addresses
22 as opposed to what a lot of spammers do; harvesting and
23 doing combinations of letters and numbers that,
24 hopefully, some are attached to real people. This
25 database would, in fact, be all true, qualified leads for

1 them.

2 MS. TREANOR: One thing that this would
3 differentiate this from the Do Not Call model is that --
4 you know, there are finite amounts of phone numbers out
5 there. The FCC comes up with the area codes and phone
6 numbers. Ultimately, you know -- you already know whose
7 name is attached to a phone number, and those are
8 publicly available in the phone book.

9 If you create a Do Not E-mail database, you're
10 kind of creating a phone book that doesn't exist right
11 now because you're going to attach e-mail names to a
12 person's identity, perhaps to their phone number, perhaps
13 to their address, perhaps their business address. Right
14 now, that doesn't exist.

15 So I think it would be immensely valuable to
16 hackers and people who are looking for personally-
17 identifiable information that, right now, they don't
18 really have, unless you have a relationship with
19 different people you're doing business with and providing
20 them with your e-mail address.

21 For our folks, if they're shipping something,
22 then you have the e-mail address, the phone number, and
23 the address. But those are rather protected lists, and
24 most of our folks don't sell that information outside of
25 their businesses.

1 MR. RICHARDS: I think another challenge -- you
2 know, we pride ourselves, as a company, on being very
3 control conscious, and there's no doubt in my mind that
4 we would follow all -- cross the T's and dot all the I's
5 and do the right thing.

6 I think there's a whole host of folks that
7 aren't going to have the technical wherewithal to
8 interface (e.g. the small mom and pop.) The small
9 business won't really have the capacity, the transmission
10 capabilities, all that kind of stuff to interface
11 regardless of whether you have a control or decentralized
12 solution.

13 Then you have the bad guys. They can still e-
14 mail around. They don't necessarily have to go to the Do
15 Not E-mail Registry. You're still going to have the
16 challenges of chasing them down.

17 I think, to Beth's point, it's a good concept.
18 I think the practical reality is, is it going to actually
19 exacerbate the situation with the bad guys, because it
20 creates, frankly, a great opportunity for them -- for
21 one-stop shopping, if you will -- for a lot of e-mail
22 addresses.

23 Another thing, with respect to e-mail
24 addresses, particularly: some companies actually use
25 those as an authentication mechanism or a password.

1 MR. SALSBURG: Can you give me an example of
2 that?

3 MS. MARSHALL: I can. On many commerce sites,
4 your e-mail address is your user ID. And you'll create a
5 password in addition to that. But your e-mail address --
6 rather than trying to create another unique number, they
7 consider the e-mail address enough to be you, so why not
8 make it half the key, if you will.

9 MR. SALSBURG: So, if you are a consumer who
10 did not generally give out his or her e-mail address,
11 this would create a security issue?

12 MS. MARSHALL: Well, it could. I mean, it's
13 part of the access to your information at web sites.

14 MR. TREANOR: I guess the way to protect that
15 information would be, instead of sending the lists out to
16 folks, us -- all of the marketers come to you, and you
17 run our suppression lists.

18 But I think that also would create a
19 bottleneck.

20 It's my understanding that to download the
21 entire Do Not Call List right now, it can take, depending
22 on different tiers, technology available, and the speed
23 at which you're working, several days. That's 60
24 million.

25 So I'm assuming that if you got that or upwards

1 of that on a Do Not E-mail Registry, it would take that
2 much time to run the entire list. Once it gets up and
3 running, you may be only running partials of the list for
4 suppression.

5 But right now, our folks have to comply with
6 that ten-day window. So I don't know if you'd be
7 envisioning having a longer or shorter period of time.

8 Congress, in an appropriations bill, changed
9 the Do Not Call Registry from a quarterly to a 30-day,
10 and our folks are already having problems with that, in
11 that it takes so long to run the list when you have to
12 run the whole thing, and that they tend to pull their
13 lists for marketing several weeks in advance of a
14 marketing campaign. Then they generally will execute a
15 campaign over several weeks.

16 So, right there, the way that they run their
17 businesses is bumping up against this 30-day requirement,
18 and they're not really sure how they're going to change
19 their businesses.

20 Right now, when someone simply opts out of an
21 e-mail, it's a much more streamlined process than having
22 to run against a list, constantly.

23 I know, at Christmas time, for instance,
24 retailers are constantly changing the promotions that
25 they're sending out. They're literally within days of

1 deciding whether or not something's going to be on sale,
2 whether or not they're going to offer an incentive, do
3 they want people in their stores or to hit their web
4 site. How do you manage that when you have to run
5 against such a large list?

6 MR. SALSBURG: What's the typical size and
7 technical sophistication of your members who are having
8 to take several days to download and scrub lists?

9 MR. TREANOR: I've heard from one our very
10 large numbers, probably one of the largest members -- and
11 they're operating without running all their zip codes --
12 that it takes them a long time. When they heard that
13 they had to go to 30 days, I think there was a lot of
14 consternation on their part.

15 And I also don't -- one thing I often explain
16 to people on the Hill when we were talking about CAN-SPAM
17 is, don't assume that just because a retailer looks
18 sophisticated from the outside that their computer
19 systems are sophisticated, because I can tell you that
20 they're not -- most of them aren't.

21 Unlike e-commerce sites or ISPs, they've built
22 their whole businesses on technology. Retailers have
23 generally gotten into this whole e-commerce thing as an
24 afterthought, and they've sort of cobbled together their
25 technology. Their databases don't necessarily talk to

1 each other at this point in time.

2 And there are companies -- and I'm not going to
3 name any names -- you would think that they would
4 probably have high-level technological expertise, and
5 they don't necessarily have it or they haven't gotten to
6 the point where they feel comfortable enough with it yet.

7 Retailers are in the business of updating their
8 cash registers every seven years, just to give you an
9 example. They don't necessarily update their technology
10 that frequently.

11 MR. SALSBURG: I would assume that -- on the
12 other hand, MBNA is probably one of the more
13 technologically sophisticated companies out there. Do
14 you have a similar experience with Do Not Call? And how
15 long would it take a company of your size, that operates
16 in all 50 states, to do a scrub?

17 MS. MARSHALL: I would say that there's going
18 to be a distinction I draw between the technology
19 associated with calling -- which has been an avenue open
20 to us for marketing for many, many years -- versus the
21 technology associated with manipulating e-mail addresses
22 that we collect, because we have not had as much time to
23 build the systems around that.

24 I'd say that we were doing 30-day updates from
25 Do Not Call from the beginning, as opposed to

1 quarterlies. So that won't, by itself, cause a
2 difficulty. But there is the same type of issue, where
3 there are elements to list preparation that are there.

4 But the ultimate medium is phone calling or e-
5 mailing. People generally believe that e-mail is
6 instant, but it's not. You're still looking at criteria
7 for selecting certain accounts, if you will, that you
8 want to talk to, and then the e-mail address is
9 associated with them.

10 When your layering-on processes of having to
11 run your selected leads against lists -- whether you've
12 got them in-house and you've got all the power to run
13 that as quickly as possible, or whether you're
14 outsourcing it, which is often the case -- that's still
15 adding time.

16 I think the ten-day requirement is problematic
17 today for e-mail, and it becomes more challenging when
18 you've got additional steps that are going to add time to
19 that. But we don't have the internal capacity for that
20 suppression for e-mail today. We outsource all of that.
21 We do it for the Do Not Call.

22 MR. SALSBURG: How different would the
23 technology for scrubbing your marketing lists against a
24 National Do Not E-mail Registry be from scrubbing your
25 lists against opt-out lists -- which you would be

1 scrubbing against, anyway?

2 MS. MARSHALL: The technology is the same.
3 It's really a big question of capacity and volume. The
4 run time is really the big variable, when you're
5 performing that work. There are other front-end and
6 back-end things in terms of file formatting.

7 But in our business model, we also have
8 individual partners' marketing lists to take into
9 account. We talk to our own customers but also do
10 marketing through 5,000 partners. So the format and file
11 sizes, imagine going from very sophisticated retailing
12 partners to very, very small organizations. So there's a
13 wide range that we're trying to account for.

14 MR. SALSBURG: Steve, do you have any thoughts
15 on this?

16 MR. RICHTER: My thoughts are, basically, with
17 the industry more centered around the skepticism of the
18 list, in that, if you go to the web sites of some of the
19 major players in this industry, like Microsoft and Yahoo!
20 and AOL, where they advise the subscribers to their ISP
21 not to opt-out; you know, when there's an opt-out link on
22 an e-mail, even after the CAN-SPAM Act, they tell their
23 subscribers not to click it because of the
24 unscrupulousness of the industry, and that if you provide
25 your name on that opt-out, as someone said earlier,

1 you're now confirming it's a good e-mail address. So
2 that's where I start, at the whole beginning here.

3 The industry doesn't support this whole idea of
4 opting out, and that is obviously what that List starts
5 with. By providing your name, you're telling the world
6 you're opting out of being in the commercial e-mail
7 listing.

8 So how does the FTC address that; that even if
9 you go ahead with a List and you have the proper security
10 applied to it and we get past the technology and the
11 security and all those issues, you still have the people,
12 who rely on their ISPs for getting mail in and out,
13 telling them not to do it -- not to opt-out?

14 MR. SILVERMAN: Wasn't there already an
15 incident where a hacker created a site or was sending e-
16 mails out claiming to be the FTC Do Not E-mail Registry?

17 MR. RICHTER: Yeah.

18 MR. SILVERMAN: You would probably expect more
19 of that.

20 MR. RICHTER: Yeah. But I think that was
21 quickly -- I think all the parties quickly resolved that;
22 the FTC and the guy who had the site.

23 But my problem is, in talking to -- you know,
24 representing a lot of people who do e-mailing -- they're
25 with the most legitimate kinds of e-mails. You know, I

1 mean, it's just take the CAN-SPAM Act and look at the e-
2 mail, and there are images and the opt-out links work and
3 there are people sitting at desks waiting for these opt-
4 outs, and it's not even one percent. It's below one
5 percent. They send ten million e-mails. They're not
6 getting ten people opting out with an opt-out link that
7 works.

8 We've talked to, like I said, the folks at
9 Microsoft and AOL and, on their web site, they have
10 posted to their new subscribers and their old subscribers
11 -- and it says, "Suggestions on how to stop spam." It
12 says "Do not use the opt-out link."

13 MR. SALSBURG: Scott, you described three tiers
14 of marketers that use e-mail: the legitimate companies
15 that are sophisticated technically; the mom and pops out
16 there who may have no bad intent; and then the spammers.

17 MR. RICHARDS: Right.

18 MR. SALSBURG: On which classes of these
19 marketers would compliance costs fall?

20 MR. RICHARDS: Well, it would be on the good
21 guys. They're going to try and comply. They're going to
22 go through the certification process -- which there's
23 some cost associated with that.

24 There are obviously costs in terms of building
25 their lists and suppressing and going against the

1 Registry. If you do it, it's going to cost a lot of
2 money to them.

3 The flip side is the mom and pop ends up not
4 using e-mail.

5 So it's a cost question but it's also a
6 competitive inequity question for the big players versus
7 the small players in the e-mail space.

8 MS. MARSHALL: E-mail is widely touted as the
9 most efficient way of finding customers. And there are
10 costs associated with it but it's certainly cheaper to
11 send an e-mail than a direct mail piece -- and faster and
12 all that type of thing.

13 But if you count added costs to that, it
14 becomes less appealing. Then if there are regulatory
15 fees or penalties associated with not doing it exactly
16 right, that's going to make it even less appealing. It
17 may be just easier to just figure out how many people you
18 can afford to direct mail than it is to figure out how to
19 comply. That's a disadvantage for them.

20 MS. TREANOR: I just wanted to bring up one
21 other issue. On the National Do Not Call Registry, you
22 can actually only call a portion of the list. You can
23 pull up your area code. So, if I'm a local retailer here
24 in the Washington area, I might want to pull 301, 202,
25 and 703.

1 I may be a local retailer who has a list of
2 people's e-mail that they are pretty sure are local e-
3 mail names. I've gotten them from other businesses in
4 the area or whatever. I've had people write their e-mail
5 addresses down when they've walked in the store.

6 How do you then differentiate if those people
7 want to send an e-mail campaign from making them pay for
8 the whole list, which may have tens of millions of names
9 on it, versus just running people in their area? That's
10 probably going to be problematic for those smaller
11 businesses.

12 You do want to use e-mail. I think that a lot
13 of people of our mom and pops have established web sites
14 now, and they really do want to get into e-mail marketing
15 just because, as Scott can tell you in a little while, e-
16 mail marketing campaigns are very successful for
17 retailers, tend to really bring businesses to their web
18 sites and to their stores.

19 MR. SALSBURG: Can that cost issue be corrected
20 by just changing the cost structure? For instance, a
21 marketer can pay per e-mail address that was scrubbed if
22 there was a centralized place to do the scrubbing?

23 MR. TREANOR: I don't know how you could set it
24 up and sort of break down --

25 MS. MARSHALL: You could scale, but to your

1 point, if all I want to do is scrub against this metro
2 area, there's no way to know that with an e-mail address,
3 unless you're asking for additional information in that
4 Registry; you know, not only tell us your e-mail address
5 but your area code or your zip or some other way to geo-
6 code the output, which may help in being able to access
7 sections of the list. But, over time -- you keep the e-
8 mail address but you move. So now it's not really
9 correlated anymore geographically.

10 MS. TREANOR: There are companies who probably
11 own lists -- even for local marketing purposes that own
12 lists of e-mail addresses. They're from the area.

13 MS. MARSHALL: Just another method would be
14 saying -- if your business has this annual profit or
15 whatever gauge you want to make, then you have a certain
16 fee structure that applies to you as opposed to companies
17 of another size will have different structures.

18 MS. TREANOR: Yeah. But then, again, even
19 large retailers -- recently -- I'm just going to give you
20 an example, Target Corp. They have their -- Marshall
21 Field's flagship store in Chicago. They had a big event.
22 There was a parade, and all sorts of stuff went on. They
23 might only want to e-mail people in the Chicago
24 metropolitan area. They may know who those people are
25 but they have to run the entire list just to make sure

1 they're not sending out an e-mail to someone.

2 You know, there are a lot of different -- even
3 nationwide retailers do have specific local needs, at
4 times, where they probably just e-mail certain folks.

5 PARTICIPANT: Any nationwide would probably
6 purchase or license the whole list, anyway, for other
7 marketing.

8 MS. TREANOR: Right. But if you're doing it
9 every ten days, I'm assuming they're going to have to
10 keep running for most -- even if you have different types
11 of marketing campaigns that you're running, you may have
12 to run the list each time just to make sure you're not
13 going to be in violation.

14 MR. SALSBURG: How much lead time do e-mail
15 marketers need? Is it like a television advertisements,
16 where several months can be spent putting together a
17 campaign? Or is it more like, somebody thinks of it and,
18 tomorrow, they want to have something out?

19 MR. TREANOR: I just know from our folks, when
20 we were discussing CAN-SPAM on the Hill, one of the
21 reasons that that ten-day period was put in as a flexible
22 ten-day period for you all to evaluate was because our
23 retail community really had a problem with that. They
24 were more comfortable with the 30-day structure just
25 because of the way that they structure their pulls for

1 marketing.

2 They plan the campaign. They do their data
3 mining; figuring out who their target customer is. They
4 go through a whole process before they actually send
5 something out, whether it's a promotion or a clip of an
6 ad they may be running on TV to their customers.

7 Most of them, in addition to that, use third-
8 parties to send the e-mail out.

9 So there are lots of steps in the process. And
10 when they were confronted with even a mandatory, hard-
11 and-fast ten-day period, it really sort of made them very
12 nervous that they would even be able to comply with that
13 in that period of time, or they were going to have to
14 restructure how they do their campaigns, completely.

15 So this is really kind of what I mentioned
16 before concerning marketing practices because just with
17 the opt-out, even the single opt-outs that are coming in,
18 and this would be for a sale. They would have to be
19 continuously running the list.

20 MS. MARSHALL: To echo your point, there's a
21 lot of preparation that's been happening during the
22 selection, and what we're trying to do is front end all
23 of that work, so that the very last thing you do is
24 suppression so you've got as big a deployment window as
25 possible.

1 We're handling the suppression for other people
2 who are deploying -- our partners, generally -- and we're
3 trying to make all of those selections up front. Then,
4 not knowing how many net leads they'll be left with, you
5 hope that what you're left with is still workable -- and,
6 generally, it has been.

7 But they may still be doing some segmentation,
8 some personalization to the ultimate message. And we
9 find that that window -- we're pushing right up against
10 the ten days today, and that's just with the sender-based
11 opt-out. We haven't layered on a second pass through a
12 different list.

13 I think, if they're both required, they've got
14 to have a combined time period or some mechanism that
15 allows you -- where do you start counting, because my
16 sender-based suppression list isn't going to be part of
17 the Do Not E-mail Registry, it's going to be separate.
18 So just mechanically, how you do both while the clock is
19 ticking, is what's hard.

20 MS. TREANOR: One of the reasons with the staff
21 on the Hill -- they were really concerned that if you had
22 that period, that was too long, and it was just going to
23 be an additional window of time in which spammers could
24 continue to spam, and they were going to spam furiously
25 within that 10- or 30-day period.

1 We tried to point out to them that legitimate
2 marketers were already honoring opt-outs. Our folks have
3 had opt-out links for several years now, and they were
4 honoring them.

5 It really is that lead time: do I already have
6 the campaign pulled, am I already running the campaign,
7 when is the campaign ending, when does it begin? We
8 couldn't speak to the practices of people who are
9 spammers, we could only speak to the practices of people
10 who are doing legitimate marketing.

11 That short a window of time was put in there --
12 the rationale that was explained was to prevent spammers
13 from spamming furiously for 30 days. It just really
14 created a lot of problems.

15 MR. SALSBURG: If a National Do Not E-mail
16 Registry was based on the Do Not Call model, and you had
17 exceptions for existing business relationships and
18 transactional messages, wouldn't most of these concerns
19 evaporate?

20 MS. TREANOR: It would be helpful to have those
21 things, I mean, if we had to go down this road.

22 I know that our folks were very involved in the
23 commenting on the National Do Not Call, and they do all
24 things that they really felt were important to have in
25 the list.

1 But I do think that there is a certain amount
2 of consumer confusion that goes along with that. I know,
3 for instance, when the Fraternal Order of Police calls me
4 at home -- I'm on the list -- and I'm still kind of,
5 like, "Oh, wait, I have to think about this. Okay.
6 They're a charity. They're exempt." And I think that
7 even with -- when you create exceptions, I think people
8 are confused by that.

9 If they're with us, we would definitely want
10 exceptions. But I think the consumers would also have to
11 understand that if they signed up for a list, it's not
12 going to stop all the e-mail that's coming into their
13 inbox. They're still going to get e-mails from MBNA
14 about their account. They're still going to get e-mails
15 from our folks about their credit accounts or about their
16 transactions or about even promotions that are coming up
17 in the store because, if you have an existing business
18 relationship -- right now, I think it's 18 months in the
19 Do Not Call context that can continue calling.

20 I think it's beneficial for businesses, but it
21 leads to confusion, too.

22 MR. RICHARDS: I think you'd still have issues
23 for new acquisitions from the standpoint of security. I
24 don't think those go away at the end of the day with an
25 EBR exemption. You still have the secured implications

1 of a central database. The government would have to have
2 a very robust security system recovery capability, and
3 operational processes.

4 Some of this is falling on the business, but
5 the government is obviously going to have some level of
6 operational requirements.

7 At the end of the day, is the customer really
8 going to be better from a technical security standpoint?
9 I think you could almost look it either way. You're
10 still going to have these same issues.

11 MS. MARSHALL: I would definitely say having an
12 existing business relationship exemption would be
13 positive, if only that there would be pieces of activity
14 that wouldn't have to go through the additional step of
15 running against a suppression file.

16 But it won't take that out of your mix
17 altogether because any business is doing two things:
18 they're finding the customers and they're maintaining
19 existing ones. So it will still be part of what you have
20 to manage. But it would just get some of the volume.

21 MR. RICHARDS: It would add clarity. It would
22 add clarity for the existing customer-part of the
23 equation.

24 MS. ROBBINS: When you were saying, before,
25 that there could be issues with security, you mean

1 security of the list -- keeping the list from getting
2 into illegitimate hands?

3 MR. RICHARDS: Right.

4 MS. TREANOR: I think that there's the question
5 as to what would constitute an existing business
6 relationship. I mean, if someone goes to your web site
7 and volunteers their e-mail address, does that then
8 become an existing business relationship, even if they
9 didn't purchase anything from you or say they're going to
10 do any kind of business transaction?

11 I know, our folks often talk anecdotally about
12 people who opt-out of things, and then realize, later on,
13 that by opting-out, they didn't get the coupons in the
14 mail or they didn't get the special promotion in the mail
15 or they're not eligible to get the Clinique bonus gift or
16 something like that. And they actually generate a lot of
17 complaints to the customer service office: "Why didn't I
18 get this?" and "Why didn't I get that?" And "It's
19 because you opted-out."

20 So there's going to have to be maybe a
21 different standard for what an existing business
22 relationship is for a web site -- or an e-mail, rather
23 than someone who calls.

24 If someone goes to your site and volunteers
25 their e-mail address, I think that's a pretty clear

1 indication that they want to get your promotional
2 materials and they want to be part of your incentives or
3 your ten-percent off coupons and stuff like that.

4 MS. MARSHALL: Well, there are opportunities to
5 say, "I want you to send me this newsletter," whether it
6 is informational-content-based or whether it's
7 advertising you want; your coupons and the like.

8 There's also the element of, "I want you,
9 Company, to send me notices about something that's
10 important to me: my checking account balance just got
11 down to \$20 and I'm going to go overdrawn." Those are
12 things that are available today and considered important
13 services.

14 In theory, that's a transactional message that
15 never has to bump up against a Do Not E-mail Registry,
16 but where is that line? If they said, "Well, gee, I do
17 want you, Company, to tell me about marketing offers from
18 time to time," but "I simultaneously put myself on the Do
19 Not E-mail List."

20 So how do I reply to that person to say, "Well,
21 I see the request. I want to help you. But until you
22 take yourself off this list, I can't do it." How do you
23 clarify those types of requests or does one supersede the
24 other? We'll have date stamps on everything.

25 It's a mixed message. I understand how people

1 might say, "Gosh, get all the clutter out of my box."
2 But, again, at times, there are these five or ten things
3 that I really want, and how do you distinguish between
4 those when I doubt that the Registry will have that level
5 of detail: "I want no e-mail, except," and then a
6 detailed list of who I want e-mail from. I didn't think
7 that was part of the model.

8 MS. TREANOR: It actually kind of raises the
9 question of them having to run the list twice. First
10 you'd run the list of names that you've got against the
11 suppression list. Then you'd run the list of names of
12 people -- then you'd have a list for those who opted-out.
13 Then you'd have to run your actual opt-in back against
14 that list to see which of your customers have actually
15 opted-in who have opted-out, but actually do want to get
16 e-mails. It's kind of extra confusing.

17 MR. SALSBURG: Steve, let me throw a question
18 to you out there on the phone. If legitimate e-mail
19 marketers are opt-in marketers or getting transactional
20 messages, would a legitimate marketer ever have to worry
21 about a List?

22 MR. RICHTER: A legitimate marketer worrying
23 about -- and worrying about the List -- I mean, a Do Not
24 -- we are opted-out list -- worrying about the List.

25 I think the only thing that the legitimate e-

1 mail marketers are concerned about are the expectations
2 of the consumer, and that somebody -- and I always hate
3 doing this to L.L. Bean. But somebody opts-out of L.L.
4 Bean, but still wants Eddie Bauer. And the consumer --
5 it just causes confusion.

6 They go to one -- they're not sure why they're
7 not getting e-mails from one retailer when they told
8 another retailer that they've opted-out. And what's
9 happened here, though, is the person who deployed the e-
10 mail received an opt-out, and then adds that name to a
11 universal list.

12 Now, a lot of people in the industry are
13 sharing their opt-out lists to scrub -- to make sure
14 there's no way in hell that person's ever going to get a
15 commercial e-mail along certain lines. Say, one of them
16 would be running apparel. That's what's happening.

17 Someone, earlier, had mentioned about someone
18 who didn't intend to opt-out, but opted-out, and that's,
19 I think, the concern about the List; that we're not going
20 to have abuse complaints about receiving e-mail. We're
21 going to have "I want to be abused" complaints; you know,
22 that they're not getting e-mail, that they don't
23 understand why they're not getting them.

24 So I think all the concerns earlier that were
25 expressed, we're in complete agreement with; about the

1 security of the List, about how the List is going to be
2 downloaded, and how long it's going to take, the
3 sophistication -- and I'll also add, the fact that the
4 major industry people, the people that control the e-mail
5 boxes -- at least in the United States -- are telling
6 their subscribers not to use the List.

7 The concerns that they have over the List are
8 on both sides: A is, how effective is it if it's used;
9 and B, if it is used, then the possibility that it's in
10 the wrong hands, and now, no one will ever believe
11 anybody about opting-out.

12 MR. SALSBURG: Could a list actually help the
13 problem that you described though, because a consumer's
14 expectation when signing up for the list would be that he
15 or she would get no unsolicited commercial e-mail?
16 Therefore they would know that they have to specifically
17 opt-in to Eddie Bauer?

18 MR. RICHTER: Here's what goes on, though. As
19 a way --

20 And, again, we talked with some other folks on
21 the compliance end of your agency, like Michael Goodman;
22 talking to him about, how does this work. And this is
23 back to the opt-out.

24 If you send an e-mail to somebody, and they
25 tell you they want to opt-out. And let's say, they've

1 just opted out of L.L. Bean, but you are deploying e-mail
2 on behalf of clothing apparel people. So you notify L.L.
3 Bean and Eddie Bauer, both, that this person doesn't want
4 e-mail regarding outdoor apparel, and even Eddie Bauer
5 having sent an e-mail to these people.

6 But out of an abundance of caution, they get
7 this list and say, "Well, we're not even going to take a
8 chance with this person over here. They've already
9 notified one of our affiliates or an advertiser that they
10 don't want e-mail from this line of production" -- you
11 know, a line of items.

12 Everyone's in agreement that that's carrying it
13 to a stretch as far as having people opted-out. But what
14 you've got here is a pendulum. The legitimate e-mailers
15 don't even want to come close to sending someone an e-
16 mail who has expressed to someone else that they don't
17 want anything else.

18 Then, on the other side, the illegitimate e-
19 mails, they're praying that the list comes into existence
20 so that they will have themselves a couple of hundred-
21 million valid e-mail addresses.

22 Our overall feeling on this is this is not a
23 time that has come with regards to this National E-mail
24 Opt-Out List. We're not as technologically capable of
25 meeting the expectations of the consumer as the Do Not

1 Call List is. I don't think you have, in the Do Not Call
2 area -- where I'm not an expert -- the number of
3 telemarketers and the number of telemarketers operating
4 out of countries that there's no cooperation between law
5 enforcement agencies and putting illegitimate
6 telemarketers out of business.

7 Where, in the e-mail industry, the real bad
8 spammers are not in this country, or at least they're not
9 operating out of this country. So how do you enforce
10 this list?

11 MS. TREANOR: If you look at sort of the e-mail
12 and its common use in the past ten years, I think a lot
13 of reasons why -- and I'm not talking about -- obviously,
14 businesses put their employees on e-mail for productivity
15 purposes. It's just a lot faster to communicate that way
16 and send documents and stuff.

17 The average consumer that has e-mail at home --
18 office or in their home, who has an AOL or Yahoo! account
19 or something like that, I think a lot of those people got
20 online initially, not only as an easy way to communicate
21 with their friends or an instant message, but I think a
22 lot of them got online because they realized that they
23 could do business online.

24 They could have their account balances e-mailed
25 to them. They could get ten percent coupons at the Gap.

1 And they were seeing their friends get the benefits of
2 those things like shop online promotions, free shipping,
3 no sales tax, all that kind of stuff, and they actually
4 opened their home accounts because it was a portal to e-
5 commerce.

6 And I think, kind of like a phone tree, over
7 time -- that's sort of the way e-commerce has kind of
8 grown. And it's really been driven by e-mail.

9 Scott has some numbers that he can show you.
10 Eighty-seven percent of all e-retailers who do business
11 online believe strongly that e-mail is their best way to
12 get to their customers; it's much better than
13 advertising, it's much better than pop-up ads. He's got
14 a whole graph to show you.

15 MS. ROBBINS: Do you mean existing customers or
16 to cultivate customers?

17 MS. TREANOR: I think it's both. When they
18 send out their (inaudible) --

19 MR. SILVERMAN: We asked them, during the
20 holiday period, every two weeks, in 2003, November-
21 December, which marketing vehicles -- whether it was
22 search engine marketing, dropping the catalogue, a coupon
23 in your web site.

24 Then their own e-mail promotions, you can see
25 87 percent, 86, 77. That was for different two-week

1 periods during the period. But it trumps everything else
2 in terms of most successful marketing vehicle for them.
3 I have copies if you want to have that.

4 And I think it's also -- you know, put that in
5 the context of the fact that online retail surpassed \$100
6 billion in 2003 -- it was over a 25 percent increase from
7 the year before -- represents about four-and-a-half
8 percent of all retail and, in some categories, like
9 computers, as much as 32 percent of all the volume of the
10 revenue dollars for those categories. And it's expected
11 to continue to increase. What the cap would be, it's
12 hard to tell. I think a lot of people would say, easily,
13 ten percent; and that's just the online transactions.

14 But the retailers are also using e-mail and the
15 online medium to drive traffic into their stores, to
16 raise the visibility about their brand. It's become a
17 very important marketing channel for them; not just a
18 sales channel.

19 So, whether it's increased cost for the
20 retailers, if it's security concerns that may actually
21 increase the amount of spam, if it's causing confusion
22 among consumers because they think they opted out but
23 they didn't, if it's slowing down their time to run e-
24 mail campaigns -- all of these things need to be taken
25 into consideration of how effective and what a driver to

1 the economy e-commerce is, overall.

2 I guess, most specifically, the biggest concern
3 of our members right now is getting their e-mails
4 delivered because they're being blocked by the ISPs or
5 they're just not being read because there are so many --
6 you know, I see that list right up there of the e-mails,
7 like that, that they're getting, and the ones that they
8 actually ask for are being lumped into those, and they're
9 just not being read. So it's become more and more of a
10 challenge for the marketers to get their message through
11 -- the legitimate marketers.

12 MS. TREANOR: But even amongst all that other
13 clutter, they are having high success rates with their e-
14 mail. We maintain that people like getting e-mails from
15 our members. People like seeing the coupons and the
16 promotions, merchandise in the stores.

17 MS. MARSHALL: Well, it's the way you interact
18 with companies you do business with these days. Not 100
19 percent of people are comfortable doing that type of
20 thing online. But, more and more, people are gaining
21 that comfort level.

22 The financial services industries use it
23 heavily. Not only is it the communication channel of
24 choice for some customers, it's a very practical, cost-
25 savings method if you can give them that statement online

1 instead of printing it on paper. The company saves
2 money. Those are ways to keep the cost low for
3 everybody. But they are showing the preference for that
4 method.

5 MR. SILVERMAN: Our research is projecting that
6 between now and 2008, each year, five million more new
7 consumers will be shopping online than the previous year.
8 So there's a tremendous amount of growth in the number of
9 people who are shopping online and communicating with
10 retailers or banks or travel companies or whatever.

11 MR. SALSBURG: So let me ask you a question
12 about your study, before we go on to another model.

13 Colleen asked about the breakdown between these
14 numbers in their study of unsolicited messages that are
15 used to cultivate new customers and e-mail to existing
16 customers. Is that explained anywhere in this data? Are
17 there such breakdowns?

18 MR. SILVERMAN: We don't have that breakdown.
19 The retailers will sometimes reach customers through
20 those that they may have an existing business
21 relationship with through e-mail. Predominantly, they're
22 reaching customers that are already -- you know, folks
23 that have opted in and they're already in their database.

24 MR. SALSBURG: Let's move on to the second
25 possible model that people have considered, which is a

1 domain wide opt-out registry. Under this model, rather
2 than the consumer submitting his or her e-mail address to
3 a centralized registry, an ISP or a business that owned
4 the domain name or an individual that owned the domain
5 name would simply list the entire domain on the Registry.

6 Why don't we talk about whether there are any
7 additional different concerns, and whether this helps, or
8 hurts from your perspectives.

9 MR. RICHARDS: Can I ask a clarifying question
10 on that?

11 MR. SALSBURG: Sure.

12 MR. RICHARDS: Do you envision the underlying
13 e-mail addresses associated with that may still be
14 captured or just the domain?

15 MR. SALSBURG: Just the domain.

16 MR. RICHARDS: I wasn't clear.

17 MS. TREANOR: Scary, I think, for our members,
18 especially since a lot of them are sending e-mail to
19 folks who have online accounts that are home based, like
20 AOL and things like that.

21 I really think that one of the things we tried
22 to balance in working on the Hill with the CAN-SPAM Act
23 was trying to --

24 The ISPs came to the Hill with a lot of asks.
25 So I think one of the things that we were very concerned

1 about in trying to draw up legislation and help the staff
2 to understand all the things that were going on up there
3 is that you don't want to create a system that inherently
4 forces retailers or bankers into essentially joint
5 marketing agreements or paying to play.

6 AOL is going to go out there and register their
7 entire domain. So, if Old Navy wants to get its e-mail
8 to their customers or advertise on their web site,
9 they're going to have to pay a premium to do that.

10 I think that part of the driving force why e-
11 mail has been so successful is it's always been sort of a
12 democratization of communications. It's very
13 inexpensive. It's easy. There's quick response time.

14 I think that when you put folks in a situation
15 where they're essentially going to be forced to do these
16 joint marketing-type --

17 MR. SALSBURG: Why don't you explain that a
18 little more? If AOL puts its entire domain on the
19 Registry, would that mean it would be illegal for any
20 marketer to send e-mail to that domain? AOL would have
21 no role in --

22 MS. TREANOR: But AOL could then say, "Well, if
23 you really want to reach our customers, now you're going
24 to have to pay ten times what you're paying now to have a
25 banner ad pop up when they go to their e-mail."

1 MR. SALSBURG: So they'd have to shift --

2 MS. TREANOR: Exactly -- the market.

3 MR. SALSBURG: -- the market.

4 MS. TREANOR: I think it would be very costly.
5 I don't know what (inaudible). But AOL owns how much of
6 the --

7 MR. SILVERMAN: I know the four major ISPs;
8 AOL, Yahoo!, Microsoft, I think Earthlink, they represent
9 I think at least 60 percent of all inboxes.

10 MS. TREANOR: So that would be so powerful a
11 tool for them to say, "If you want to get to our
12 customers" --

13 MR. SILVERMAN: They might want to sell more
14 pop-up ads or other advertising that may be considered
15 even more interesting.

16 MS. TREANOR: Or they'll send your e-mails to
17 our customers -- you'll get an e-mail from Yahoo! -- and
18 they do it now; they do joint marketing with companies.
19 You'll get an e-mail from Yahoo! Shopping, and Yahoo!
20 Shopping will say, "There's a great deal at the Gap.
21 Click here and go."

22 I don't necessarily think that that would make
23 -- I would assume that they wouldn't have the Do Not E-
24 mail applied to their e-mails, so that customer --

25 MR. SALSBURG: Isn't it still a concern if a

1 domain wide registry had an existing business
2 relationship exception?

3 MS. TREANOR: I think that it would be
4 interesting. I think the burden of proof -- proving to
5 the ISP that you have an existing business relationship -
6 - there would be a hurdle there, I think.

7 MS. ROBBINS: What if a domain had two domains;
8 so AOL had an "I Love Spam" domain and an "I Hate Spam"
9 domain, so a consumer could choose whether they want to
10 get on one or the other. Then marketers could send to
11 the one that allows spam or allows unsolicited e-mails.

12 MS. TREANOR: It's implying that
13 commercial e-mails from retailers are spam.

14 MS. ROBBINS: I meant unsolicited: rather than
15 permission-based or transactional messages, but
16 unsolicited messages for a marketing campaign.

17 MS. TREANOR: So people would essentially have
18 two accounts.

19 MS. MARSHALL: Putting the burden on the ISP to
20 have its own sub-registry of, you know, here are the
21 people who I will allow -- and maybe that --

22 MS. TREANOR: And they do do those.

23 MS. MARSHALL: ISPs have filters that are there.
24 I'm going to accept e-mail from exactly these "from"
25 lines. But I say that's going to be challenging for

1 them. And it's going to change every day for all of
2 their members.

3 I would wonder if there's a right of the
4 individual within that domain to reverse the order; to
5 say, "Okay, this whole domain is off limits, except me,
6 because I've opted back in. Take me off the list."

7 I can see a small business might say, "We can't
8 handle the burden, and this is not a personal e-mail
9 account, anyway, so you shouldn't have any issues with
10 it.

11 But with the larger ISPs, I think people do
12 different things with their accounts.

13 MS. TREANOR: The other question I have, too:
14 Is it technologically possible to differentiate between a
15 commercial e-mail and a personal e-mail? I know that the
16 ISPs struggle with this every day in their blocking. A
17 lot of them are not even sure what they're blocking. It
18 just looks to them like it might be spam, so they block
19 it.

20 So, then, how would you not get sort of
21 personal communications kind of wrapped up in that?

22 MR. RICHARDS: They look at key words is all.

23 MS. TREANOR: But a spammer could mask a spam
24 to look like a personal e-mail, too.

25 MR. RICHARDS: Right.

1 MR. SALSBURG: You assumed, in this model, that
2 the ISPs actually wouldn't use this data for filtering.
3 This would simply be a method for marketers to scrub, and
4 then there would be FTC enforcement. Does that change
5 your concern?

6 MS. TREANOR: If AOL or any of the big ISPs
7 just decides to take their whole domain name down -- I
8 don't know. I can still see the scenario in which it's a
9 card that they're playing, and they're playing that card
10 either to prevent spam, but they're also going to play
11 that card to -- their web site then becomes more
12 desirable, advertising space then becomes more desirable,
13 their joint marketing agreements then become more
14 desirable.

15 MR. SALSBURG: Let me ask a more basic
16 question. From the National Retail Federation's
17 standpoint, if a retailer sends an unsolicited commercial
18 message to somebody that the retailer has no existing
19 business relationship with -- it's not transactional,
20 it's advertising -- is that spam?

21 MS. TREANOR: Our folks don't believe that
22 they're spammers. They've all been including opt-out
23 links forever, and they've honored them, so that when a
24 person gets that first UCE, and they don't want any more,
25 they're off the list.

1 MR. SALSBURG: So just under CAN-SPAM, the
2 first bite isn't spam; it's subsequent ones in violation.

3 MS. TREANOR: Yes. The CAN-SPAM Act actually
4 very much mirrors what their existing business practices
5 were already. But they didn't have liability, time
6 periods, and stuff like that.

7 MR. SALSBURG: So your concern with any of
8 these models that we've talked about so far is that the
9 first bite is gone -- essentially, we've gone from an
10 opt-out system to an opt-in system?

11 MS. TREANOR: We're not even going to have a
12 chance to touch that consumer and get our product out
13 there, something that they might really want. And if
14 they don't want it, they can just opt-out.

15 MR. RICHARDS: There was a comment I was going
16 to make when we were talking about the whole telephone
17 versus e-mail channel. It is much more a customer
18 choice-driven channel than the telephone model.

19 So, when you try and analogize them, you have
20 to be a little bit careful. You don't want to just take
21 the customer's decision away, and their capabilities,
22 because that's kind of indigenous to the Internet model,
23 the customer choice aspect. They have more control in
24 the Internet space.

25 MS. MARSHALL: And if you believe that opt-out

1 works. They have that capability now at the sender
2 level. And if you get to the precision of saying, "I
3 want e-mail from L.L. Bean but not Eddie Bauer" -- as an
4 example -- instead of it being some category-wide -- I
5 don't even know how you decide outdoor apparel as a
6 category and who that applies to. But they have that
7 power today.

8 Now there may be issues in how effective it is
9 and whether it works the same for everybody. But, I'll
10 tell you, our opt-out works. We make sure it does. You
11 never get e-mail again. And I would say that most
12 legitimate players do the same.

13 MR. COLLINGWOOD: It's a small but important
14 point on what she's talking about here. One of the
15 things that distinguishes company-based opt-out lists
16 versus the Do Not Call List -- first, for example, is,
17 when you create a National Do Not E-mail List, you're
18 creating something of extraordinary value to criminals
19 and extraordinary value to illegitimate spammers because
20 you're creating this sort of massive list of legitimate
21 e-mail out there, some portion of whom will belong to
22 children -- because that's one of the biggest reasons why
23 people will opt-out.

24 And people who are illegitimate and criminals
25 will do everything within their power, technically, to

1 glom onto that list. And the same argument could -- even
2 though I'm not a techie -- even go down to the domain
3 aspect of it, where they know, if they get ahold of that,
4 they've got something of value that they didn't have
5 before, and that's entirely different from the phone
6 number.

7 MR. RICHARDS: The thing about the bad guys is
8 you're always catching up with them technically. What
9 you might put in place on Day 1 is secure enough. Six
10 months later they're going to be ahead of you from a
11 security perspective.

12 You've got to be ready to play that game with
13 the bad guys because they're not going to stand still.
14 They're going to continue to improve their ability to get
15 around your security.

16 That's what happened with encryption. The
17 reason encryption standards kept changing was because
18 each time industry would arrive at a different level of
19 encryption, the bad guys would figure it out. Industry
20 had to go to another level. That will be the reality of
21 any type of Registry that is established.

22 MR. SALSBURG: Steve, I just want to make sure
23 you have a chance to speak here on domain wide registry.

24 MR. RICHTER: The concept appeals to me because
25 I think it actually is one way of having people, at least

1 with the consumer, understand that they're now going into
2 a "No Unsolicited," if you will -- or "-Solicited"
3 commercial e-mail world.

4 But the problem, again, as one of the speakers
5 just said, is the security. It's the unrealistic
6 expectations that they're going to get what they're
7 asking for.

8 MR. SALSBURG: Which means compliance would be
9 low?

10 MR. RICHTER: Yeah. You know, what I'm seeing,
11 since the inception of the CAN-SPAM Act, is that the
12 legitimate e-mailers are more legitimate now. They have
13 gone out of their way to make sure that every single item
14 in that CAN-SPAM Act is complied with, and vigorously.
15 And it almost looks to me like the illegitimate spammers
16 have said, "Now we can raise holy hell like we've never
17 raised it before."

18 I notice on -- all of our associates have on
19 their e-mailing -- they have their own spam traps to see
20 if the people they're hiring are sending out spam. And
21 there's never been more spam before. There's more spam,
22 now, since the CAN-SPAM Act than there was before. It's
23 worse. It seems to be bolder, as far as what they're
24 selling and passing the point of obscenity.

25 I hate to say what someone else said before,

1 but I think so much of whatever model we come up with is,
2 what is the FTC capability going to be to, not so much
3 make sure that the people who are trying to comply are
4 complying, but to punish the people who are blatantly
5 abusing the system. And, of course, that gets down to
6 budgeting constraints for you.

7 MS. TREANOR: And I think what a Do Not E-mail
8 list is not going to do is it's not going to block. The
9 legitimate folks are going to come and they're going to
10 run their lists. They're not going to e-mail those folks
11 on the list.

12 But it's not going to block spammers from
13 sending e-mail. So, if they get ahold of the list or
14 they continue to harvest and do whatever they do, they're
15 still going to be able to send their e-mail. And unless
16 the ISP can recognize them and block them, they're still
17 going to get through.

18 Interestingly, too, we had this problem in NRF.
19 All of our e-mail addresses are on our web site, so
20 people were harvesting names and we were getting a lot of
21 spam in our inboxes. So our IT guy went out and
22 purchased a blocking system.

23 Our e-mail spam went down, but they didn't go
24 down a whole lot, especially in the first kind of few
25 months. But the e-mails that were getting blocked were

1 actually from our members because all these filters put
2 common retailers who send a lot of e-mail, whether it's
3 spam or not -- they just send a lot.

4 So we weren't getting e-mail from a lot of our
5 members. They were being blocked by our blocker. They
6 were legitimate e-mails that were being blocked. The
7 illegitimate ones still weren't being blocked. And until
8 we kind of perfected the system, we were having some
9 problems.

10 And I think the same thing is going to happen
11 here. The e-mails are still going to go through. And
12 the common folks who send a lot of e-mails that are
13 legitimate or to people who they have customer
14 relationships with may still just be getting blocked.

15 MR. SALSBURG: You described earlier, the
16 database management costs and scrubbing costs if there
17 was a Registry of, let's say, 300 million individual e-
18 mail addresses.

19 How do those costs and the technical
20 sophistication needed to do scrubbing change if, rather
21 than scrubbing against a list of e-mail addresses, you're
22 scrubbing against a much smaller list of domains of,
23 let's say, 30- or 40,000 domains?

24 MS. MARSHALL: Well, you still have to compare
25 it against every name that you're planning to mail. But

1 I think that it would take less time if you knew that you
2 were going to knock out every AOL or Yahoo!. I think it
3 would take less time.

4 But there is still an expense for someone to
5 perform that task and for file formatting. Those things
6 won't change. But, by nature, it would be a shorter
7 list, if you will.

8 MR. SALSBURG: From a retailer's perspective,
9 if they're not sophisticated, is the same infrastructure
10 needed to do scrubbing no matter whether it's a domain or
11 individual e-mail address Registry?

12 MS. TREANOR: I believe so. I know that for
13 telemarketing -- I think a lot of small businesses that
14 are doing it, they're hiring third parties to do it
15 because they don't have the resources to do it. So
16 (inaudible) handling something that maybe you could have
17 handled internally, before, but you can't handle
18 internally anymore.

19 MR. SALSBURG: Anyone have final thoughts on a
20 domain wide registry, before we move on?

21 (No response.)

22 MR. SALSBURG: Let's throw out a third possible
23 model; and that would be similar to the first model, a
24 registry of individual e-mail addresses. But to
25 alleviate the security concern of the list getting into

1 the hands of a spammer, the list would be kept by one or
2 a limited number of organizations that went through an
3 approval process with the FTC. We kind of knew who they
4 were, knew what kind of security precautions they would
5 keep on the lists, et cetera.

6 A marketer would forward its marketing list for
7 each campaign to this third party, which would do the
8 scrub, and then only forward on those e-mails to
9 consumers who were not on the Registry.

10 MS. MARSHALL: That's a model that we follow
11 today for our own sender-level suppression file. I'd say
12 that the friction points are, what is the security
13 guarantee when I put my list somewhere? I think there
14 need to be standards on what level of review are these
15 vendors under, how frequently are they reviewed, what is
16 the scope of that review.

17 Because we're turning over a very valuable
18 asset to a third party with whom, I'm guessing, we have
19 never dealt before. And we generally take on that review
20 ourselves, and it's very vigorous and detailed.

21 We would assume the same level of vigor from
22 the FTC or whomever if certain vendors have been
23 designated. I think that their level of security, their
24 pricing, and what the turnaround times are going to be
25 are all critical.

1 Part of the security would be, how are files
2 transmitted, how are they handled, how are they returned,
3 the passing of encryption keys, FTP as a transfer method
4 -- but being able to accommodate other media because
5 there are people who are not conversed in that method.
6 So how do you handle disk input-disk output?

7 And what are individual users' avenues for
8 researching problems? You know, "I got back a file that
9 doesn't resemble what I gave you" or "You gave me
10 somebody else's file." What are the processes for
11 pursuing those problems and getting satisfaction?

12 MR. SALSBURG: You said that you do this
13 already. I guess that means -- correct me if I'm wrong --
14 - that you don't actually send out, physically, the e-
15 mails to your customers. You use a third party for this?

16 MS. MARSHALL: Right. Actually it would be
17 considered two halves. But we talk to our own customers.
18 We're definitely using a vendor to prepare the list. And
19 they have access to our suppression files so that that
20 step is performed.

21 When we market on behalf of our partners, they
22 are generally doing the deploying. In the past, we never
23 saw the list. We'd give them marketing materials and
24 they would send it on our behalf. Today, we have to see
25 their list because they have to come in the one door

1 where our suppression file is.

2 They are coming very reluctantly. They have
3 all the same concerns that I would have in their place;
4 which is, "I'm giving my list to whom?" and "What's going
5 to happen to it?" "What guarantee do I have that it's
6 not going to be compromised or used or altered in some
7 way that is unacceptable to me?" "Who are these people?"
8 "Where is my list going?"

9 We're able to overcome those objections because
10 we can answer all the concerns. I would ask the very
11 same questions of the place where I would send my list:
12 "How is it going to be treated?" "What are the security
13 features, turnaround times, and cost?"

14 MR. SALSBURG: Based on your experience then,
15 what kind of turnaround do you expect when you're doing
16 this on the small-scale -- one company engaged in this
17 practice?

18 MS. MARSHALL: Well, today, 48 hours would be
19 the standard. I think that that's a challenging
20 expectation if you've got a limited number of vendors
21 that are attempting to perform this function for every
22 marketer in the country.

23 So I think a reasonable time, to me, would be
24 48 hours, but it may need to be longer just because of
25 the run time.

1 MS. ROBBINS: How do you assess the security of
2 the list? How do you know that the party that you're
3 using is keeping the list secure? What things do you
4 base that on?

5 MS. MARSHALL: We have separate teams of people
6 who go in and assess vendor security. But it ranges from
7 how information is transferred to and from, how secure --
8 encrypted it is the physical security of the location
9 where the information is being manipulated -- from are
10 there ID badges used for every person who can go in and
11 out of the building, to what are the technical security
12 elements of where the information is housed -- how can it
13 be protected from hackers and that type of thing; a wide
14 range of things.

15 MR. RICHARDS: We'll do penetration tests and
16 give them feedback. And if their security isn't up to
17 our standards, then they have to make certain changes.
18 It's our information security folks that know how to
19 really test their security.

20 The tie-in is, you can distribute the load, but
21 you can't distribute the security standards. They're
22 still going to have to be the same, whether it's a
23 central or distributed registry.

24 The other thing is, you'd have to work through
25 the file synchronization challenge. You have to make

1 sure everybody is getting the same updates at the same
2 time. It's not saying that you couldn't do it, but those
3 are going to be overhead requirements in that kind of
4 model.

5 MR. SALSBURG: Is your focus on security, not
6 just to protect the value of your marketing list, but
7 because the content of some of these messages are
8 transactional? They are credit card statements and --

9 MS. MARSHALL: Well, I wouldn't see that the
10 location or the center for scrubbing would have any of
11 our e-mail content. They're getting e-mail address,
12 only.

13 Now we see situations where there are other
14 fields associated with it, maybe a unique identifying
15 number, so that e-mail address can be mapped back to your
16 lists so we can personalize your e-mail.

17 MR. SALSBURG: So they return to you to scrub
18 lists when you send out the e-mail?

19 MS. MARSHALL: Yes. In terms of the content,
20 like your credit card number, I wouldn't see a list
21 processor having that.

22 MR. SALSBURG: If, in this forwarding service
23 model, the forwarding service actually was sending them
24 on with the e-mail, would there be an additional concern
25 because they could see the content?

1 MS. MARSHALL: We're not participating in a
2 model like that today.

3 MR. SALSBURG: Right. I'm just describing it.

4 MS. MARSHALL: I would say, in general, our e-
5 mail content is never going to have information that's
6 that critical because it's unsecure. We're not going to
7 transmit your entire account number, your Social, your
8 balance, and "By the way, you're past due." That's not
9 going to be the content of the message.

10 MR. RICHARDS: By the same token, I think part
11 of the reason for doing the penetration test is that we
12 view the information as sensitive. In real world terms,
13 we consider it something we should do, and it's important
14 that our customers know we feel that way.

15 MR. SILVERMAN: The turnaround time strikes me
16 as a really important issue. Just look at the last
17 holiday season. There were price wars for toys, where
18 one retailer was reacting to another retailer or saying
19 they found out that one retailer didn't -- they ran out
20 of inventory of one thing and they want to capitalize on
21 that, somehow.

22 If it's slowing down the process, they have to
23 send it to a processor to get it forwarded. It could
24 water down a competitive advantage that they may have.

25 MR. SALSBURG: Elizabeth, you described before

1 that a lot of e-mail marketing campaigns are long in the
2 works. There obviously must be some instances, then --

3 MS. TREANOR: Yeah, during the holidays, they
4 can be very reactive. But they often do -- they just
5 plan campaigns way ahead of time, just like they do
6 commercials that are going to run on TV and things like
7 that.

8 But one of the things I see in this whole
9 situation with the forwarding service is that a lot of
10 their folks do use third parties, like MBNA does, and
11 they probably actually spend a lot more on their content
12 out with them to the third parties, as well, because
13 they're not sensitive at all.

14 I would actually be concerned about you would
15 end up, inadvertently, putting one of these ESPs sort of
16 out of business. There are some really good firms out
17 there who do really good work and are very well
18 respected. They're very anti-spam. I would be concerned
19 that you were affecting these folks.

20 MR. SALSBURG: You'd be creating an oligopoly?

21 MR. SILVERMAN: In addition, these ESPs compete
22 by adding more functionality, helping the retailers
23 segment their lists, helping them accurately measure the
24 performance of their e-mail campaigns. I think it's
25 really important that that remain a competitive

1 environment that the retailer can choose the ESP based on
2 how much they're going to enhance their ability to make
3 their e-mail campaigns as effective as possible.

4 MR. SALSBURG: Scott, you raise a very
5 interesting point. Let's say, the forwarding service
6 sends along only those e-mails to people who are not on
7 the list. From a marketer's standpoint, if you don't get
8 back information about who your messages are being sent
9 to, how does it affect your ability to plan future
10 campaigns?

11 MR. SILVERMAN: Say the question again.

12 MR. SALSBURG: I imagine, right now, when a
13 member of your organization sends out marketing e-mail,
14 they know who is receiving it. They've got a good sense
15 and they can readjust their lists for the next campaign.

16 If this information doesn't come back to you,
17 because your e-mails are all being sent through a
18 forwarding service and there's no feedback coming back
19 the other way, what kind of effect does that have?

20 MR. SILVERMAN: Disaster. You collect so much
21 data from understanding what people click on; you see
22 what kind of merchandise they're interested in, you can
23 track which customers contribute greater profit margin to
24 you.

25 These are all tools to help you focus on

1 segments that are going to: one, make it more convenient
2 for the customer because you can deliver to them what
3 they want based on understanding what their preferences
4 are; and, as a business, make sure that you're not
5 wasting marketing dollars or wasting resources on
6 customers that aren't going to be your best customers.

7 That data is critical to their business. I
8 think anything that takes that data away -- they would be
9 very -- that would really put a damper on their business.

10 MR. SALSBURG: Does anyone have any other
11 thoughts on the forwarding service model?

12 (No response.)

13 MR. SALSBURG: Why don't we move on to a fourth
14 model. This model would take the consumer out of the
15 picture entirely. It would be a registry of
16 authenticated marketers.

17 Under this model, an e-mail marketer would
18 register with the Commission, would obtain a registration
19 number, and would also list with the FTC the IP addresses
20 and domains from which it would be sending outbound
21 marketing messages.

22 The registration numbers that the marketer
23 obtained from the FTC would need to be embedded in the
24 headers or elsewhere in their commercial e-mail. The
25 ISPs and other domain owners would have access to this

1 FTC database of registration numbers and outgoing IP
2 addresses and could then adjust their filters so that, if
3 the IP wanted to, it could reject any e-mail that did not
4 have a registration number that matched the IP address.

5 Essentially, it's a method of authenticating
6 who the senders are. Any thoughts on that type of
7 Registry?

8 MS. TREANOR: We've kicked the idea of
9 authentication around. In some discussions we've had
10 internally, they've been for doing it for Better Business
11 Bureau stamp of approval on that. You kind of get an
12 agreement from the ISPs that anything that has that stamp
13 of approval on it, from NRF or something like that, would
14 be able to get through. So we would have, like, the best
15 practices retailers out there.

16 I think, from a practical standpoint, it's not
17 nearly as objectionable a format as some of the other
18 ones are because I think, then, as a legitimate marketer,
19 you feel like you're being treated like a legitimate
20 marketer, and you're able to reach your intended
21 customer.

22 But there are also problems inherent in that.
23 I guess security -- again, people -- e-mail (inaudible)
24 getting ahold of these embedded marks, you know, whatever
25 they are, and figuring out the system again. I don't

1 know the technology.

2 MR. RICHARDS: You would have to get the
3 technical guys to speak to this.

4 To me, there are two angles on that. One is, I
5 come in the door and I go through the certification
6 process. I look completely legitimate to you. I give
7 you my driver's license. I give you all the stuff --
8 "Here's my financials. I'm a solid guy" and everything.
9 You set him up and you give him your security. I'm in
10 the door. So that's one.

11 The other is where they attempt to compromise
12 security. You're going to have to build a really robust
13 authentication mechanism to make that work.

14 MS. MARSHALL: Plus, I think there's the
15 challenge of putting anybody in the shoes of saying,
16 "Who's going to be the legitimate marketer" because there
17 are things that can be legitimately marketed that may not
18 be acceptable to some people: "I don't like their
19 product, therefore I don't want you to be a legitimate
20 marketer." What's the criteria for that?

21 And maybe some people don't want to hear about
22 loans. So there's still going to be that disconnect
23 between marketers who are legitimate and people's
24 personal preferences about which legitimate marketers
25 they want to pick from.

1 MR. SALSBURG: So maybe it would be better to
2 have this registration number hidden, and have it say
3 "FTC approved" and then have there be some that are
4 "objectionable"?

5 MS. MARSHALL: That's an interesting position
6 to put yourself in, to look like you're now endorsing the
7 content of -- if the matter is considered legitimate.
8 Are they a real business? Do they have a tax ID number?
9 But maybe we still don't like what they're selling.

10 MR. RICHARDS: That still doesn't preclude the
11 bad guys from just not coming through the door.

12 MS. MARSHALL: Well, if a registry number is
13 what's necessary for delivery, and anybody legitimate
14 will say, "Sign me up. I want one." But if it can be
15 faked, if it can be stolen, if it can be mocked up, there
16 will be people who do it. So how do you distinguish
17 those or how do the ISPs tell the difference?

18 MR. SILVERMAN: It's an interesting model. It
19 hinges on the ISPs honoring the authentication or saying,
20 "Okay, it's authenticated, so I'm going to let it go
21 through." They don't have to -- you know, unless there's
22 some requirement that they have to do that, they could
23 still continue to be more aggressively blocked, like they
24 currently are doing.

25 There have been discussions about some private

1 registry models along the same lines, and there hasn't
2 been a consensus among the ISPs that they would even
3 comply with those where I think the rules would be even
4 more stringent than what the law is right now.

5 So it all depends on whether the ISPs would
6 honor it or not, in order for it to be effective.

7 MS. ROBBINS: Could you give an example of what
8 you're talking about?

9 MR. SILVERMAN: There would be maybe a non-
10 profit registry form, and it says "We have these certain
11 rules that you need to comply. If you opt-out or your
12 list is double-opted out" or whatever the rules might be,
13 "You need to pay to be authenticated." It adds that
14 authentication code.

15 If the ISPs are set up in such a way that if an
16 e-mail comes in and includes the authentication code,
17 they say, "It's good," and it's going to bypass our spam
18 filters and go to the customer.

19 That's what I think is essentially this model,
20 right? -- whether it be the FTC that would be the central
21 registry rather than having a series of private
22 registries out there

23 MS. TREANOR: The e-mail service providers were
24 working on a project called Project Lumos.

25 MR. SILVERMAN: Project Lumos is that model.

1 MS. TREANOR: I don't know if you've heard
2 about this or not. I think Trevor Hughes testified,
3 actually, to the Senate Commerce Committee -- I think he
4 talked about this a little bit. But they haven't reached
5 any consensus with any ISP.

6 MR. SILVERMAN: I think there is an
7 authenticated e-mail group that has recently been formed,
8 and they had a meeting, I believe, in the fall.

9 MR. COLLINGWOOD: Arguably, though, you could
10 make the argument that this would make the existing opt-
11 out procedures in the CAN-SPAM Act far more valuable
12 because anything that would filter out any or some
13 portion of the illegitimate, illegal spam that's out
14 there cuts the volume down, and would make the other opt-
15 out process more valuable to consumers, or more
16 practical, because they would be able to opt-out, you
17 know, marketer by marketer, and have a larger impact on
18 the volume of spam.

19 MR. SALSBURG: Would it make the opt-out
20 provisions of CAN-SPAM easier to enforce?

21 MS. MARSHALL: Well, if you connected, let's
22 say, violations back to -- you know, this can erode your
23 authentication or we can take it away. I think it would
24 put some teeth in it. But it would still be a question
25 of determining what are those levels and the research on,

1 are those legitimate complaints or is there research that
2 shows, "Hey, you did everything you could to suppress
3 people"?

4 MR. SILVERMAN: The technical premise -- I'm
5 not a technology person, but if the technical premise
6 behind this model is, the problem of spam is that the e-
7 mails can't be tracked back to a real company or person
8 that you can take action against if they're breaking the
9 law or sending something offensive -- that's the whole
10 idea: if you can just simply authenticate e-mail, that
11 might completely resolve the problem. But it's a lot
12 easier said than done.

13 MS. TREANOR: If the ISPs would honor enough of
14 it. I know some of our folks have problems with blocking
15 because national retailers, when they send out a
16 campaign, they may send out millions. It may be one e-
17 mail, "Ten percent off," but it might go to millions of
18 people. And when the ISPs start seeing that kind of
19 volume coming in to their customers, they start blocking
20 them. So, if you could get -- if you could bypass the
21 blocking system -- because blockers look for key words,
22 but they also look for the numbers of e-mails that are
23 coming in. Whereas, someone who may have stores in 50
24 states have a ton of consumers that they're going out to,
25 they're being watched just for volume; not for content.

1 It would probably help.

2 MR. SILVERMAN: We have members that have 100
3 percent opt-in lists, and they've never done e-mail
4 (inaudible), they've never -- you know, 100 percent opt-
5 in. The only way you can get on that list is if you go
6 to their web site and sign up, and they're still being
7 blocked by the ISPs.

8 MR. SALSBURG: Some of the major ISPs --
9 Microsoft, AOL, Yahoo! -- have announced separate
10 authentication mechanisms: Microsoft with Caller ID for
11 E-mail and AOL with SPF and Yahoo! Domain Keys. Then
12 there are about 1,500 other ISPs.

13 From a marketer's standpoint, would it be
14 easier to operate in the e-mail environment if there was
15 a single standard for authentication?

16 MR. RICHARDS: Yeah. That's where I was going
17 to go. I think you have to get to a standard to support
18 that model. It seems like you would. I'm not sure how
19 you would authenticate through 1,500 different kinds of
20 approaches.

21 Can you get the Microsofts to agree on a
22 standard that gives you the Good Housekeeping seal as a
23 marker? I think you still have the challenge of deciding
24 what is a good marketer versus a bad marketer. But at
25 least you've lumped a lot of good guys together.

1 MS. MARSHALL: And there could be a
2 differentiation. Let's say, your ISP says, "Here are e-
3 mails from legitimate marketers, but they don't happen to
4 be in your favorites list" or whatever -- list of your
5 caller ID, if you will, that you've created. You might
6 say, "I've signed up for e-mail from them," so they're on
7 one list. But then, "Here's e-mail from people that we
8 consider legitimate, and anything else, we throw away.
9 We won't even send it."

10 But you can make a choice on that other element
11 of legitimate marketers.

12 MR. COLLINGWOOD: I would think a Registry
13 would give you a hugely effective enforcement tool. It
14 may only be effective against legitimate marketers, but I
15 think it would be a hugely effective enforcement tool.
16 Nobody's going to want to risk losing that certification
17 -- no legitimate company.

18 MR. RICHARDS: Right.

19 MR. SALSBURG: Does anybody have any other
20 thoughts on this model?

21 (No response.)

22 MR. SALSBURG: How about any other creative
23 approaches that we haven't discussed for solving spam or
24 creating some sort of Registry?

25 MR. RICHARDS: I think they're all good ideas

1 but the technical practicality in the Internet space is
2 that the technical wherewithal isn't out there yet to
3 fulfill the theory with each model. Can you practically
4 do it on the scale we're talking about?

5 MR. SILVERMAN: And stay ahead of the bad guys
6 and their technical wherewithal, which, obviously, must
7 be more sophisticated.

8 MR. COLLINGWOOD: We haven't talked about the
9 technical disposition of techniques, like spoofing and
10 all the other things that illegitimate marketers can use
11 to block out e-mails going from legitimate marketers to
12 people, knowing full well they'll end up with a pool of
13 people who don't know they have been opted-out, they will
14 continue to spam them, where everybody else will quit
15 sending stuff like that.

16 MR. SALSBURG: Any other final thoughts?

17 MS. TREANOR: From our point of view, I think
18 that e-commerce is going to be wildly successful for
19 retailers. I think, between folks who actually do do
20 shopping online and who actually do research online and
21 then go purchase from the stores, this will be valuable.
22 I know their efforts -- they really don't want to lose
23 this tool.

24 MR. SILVERMAN: I'll go as far as to say it's
25 the lifeblood of a company that's doing business online.

1 And, if you talk to them, the notion of having e-mail not
2 be available to them because the spam problem is out of
3 control or whatever the issue is, is really -- creates a
4 tremendous amount of angst among them.

5 And the customers like being communicated with
6 via e-mail. They like receiving notices about sales or
7 new pieces of merchandise and things like that. And if
8 they lose that communications mechanism for them, it
9 would really be destructive towards their business.

10 MS. TREANOR: The brick-and-mortar folks, who
11 now are the brick-and-clicks, a lot of them really
12 reluctantly got into this whole Internet business. The
13 Internet folks will tell you that they were always
14 relegated to the basement.

15 About three or four years ago, the CEOs started
16 noticing that they were really driving business into the
17 stores, this is working out really well. Now it's going
18 to be 5 or 6 percent of the retail market next year.
19 That's extraordinary, if you think, it's only really been
20 between five and ten years that people had really started
21 using the Internet for things like shopping.

22 MR. SILVERMAN: I didn't include a slide, but,
23 of the \$100 billion, about three-quarters of that are
24 from what we call multi-channel retailers; those that
25 operate, not just online, but they may also have stores

1 or catalogues. The majority of this revenue is not
2 coming from these brand new e-commerce players. It's
3 spread out through a lot of the incumbent retailers, as
4 well.

5 MR. SALSBURG: Thank you all so much. We
6 really appreciate your taking the time to come meet with
7 us and talk with us -- Steve too. This has been
8 incredibly informative. Thank you.

9 (The meeting was concluded at 11:25 a.m.)

10 * * * * *

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

