

FEDERAL TRADE COMMISSION

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

I N D E X

INTRODUCTION	PAGE
BY MR. DAVIS	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
)
-----)

TUESDAY, JULY 26, 2005
AM SESSION
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

The above-entitled matter came on for
conference, pursuant to agreement, at 10:05 a.m.

1 APPEARANCES:

2

3 ON BEHALF OF THE FEDERAL TRADE COMMISSION:

4 MICHAEL DAVIS, ESQ.

5 CATHERINE HARRINGTON-MCBRIDE, ESQ.

6 ALLYSON HIMELFARB, INVESTIGATOR

7 LOU SILVERSIN, Economist

8 HAJ HADEISHI, Economist

9 600 Pennsylvania Avenue

10 Washington, D.C. 20058

11

12 ALSO PRESENT VIA TELEPHONE:

13 STEVE ADKINS, SamSpade.org

14 MICHAEL DELLA PENNA, Bigfoot Interactive

15 JORDAN COHEN, Bigfoot Interactive

16 CHRIS LEWIS, Nortel Networks

17 ERIC CASTELLI, LashBack LLC

18 JOHN LEVINE, IETF, Anti-Spam Research Group

19 REBECCA LIEB, Clickz.net

20

21

22

23

24

25

P R O C E E D I N G S

- - - - -

1
2
3 MR. DAVIS: Thank you so much. Good morning
4 everyone. This is Mike Davis. I'm a lawyer at the
5 Federal Trade Commission in Washington, and for the
6 first hour of this call, our colleague, Katie
7 Harrington-McBride, is unable to join us. We expect her
8 to come in about halfway through this two-hour long
9 telephone conference. When she does arrive I will
10 announce her arrival.

11 I would like to check right now to see if
12 Debbie, our court reporter, is on the line.

13 MS. MAHEUX: Yes, I am, Mike. Thank you.

14 MR. DAVIS: Great, Debbie. Debbie is our
15 reporter with for the record, and she will be on the
16 line to take down everything that we say.

17 I would also like to just do a quick roll call
18 of the conference call to see if everyone we were
19 expecting is on the line. So may I start by asking if
20 Steve Adkins is here?

21 MR. ADKINS: Yes, I'm here.

22 MR. DAVIS: Good morning. Michael Della Penna?

23 MR. DELLA PENNA: Here.

24 MR. DAVIS: Thank you, Michael. Jordan Cohen?

25 MR. COHEN: Yes, here.

1 MR. DAVIS: Good morning. Chris Lewis? Is
2 anyone from Nortel Networks on the line? Okay. Chris
3 may then join us shortly, I hope.

4 How about Eric Castelli?

5 MR. CASTELLI: Castelli, yes, here.

6 MR. DAVIS: Good morning, Eric. Sorry about
7 that.

8 MR. CASTELLI: That's all right.

9 MR. DAVIS: John Levine.

10 MR. LEVINE: Hi there.

11 MR. DAVIS: Hi, John, good morning. I also
12 believe we may be joined by Rebecca Lieb.

13 MS. LIEB: Yes, hello.

14 MR. DAVIS: Good morning. Is anyone else on the
15 call?

16 MR. SILVERSIN: Lou Silversin from economics.
17 I'm here, Mike.

18 MR. DAVIS: Great, Lou. That's Lou Silversin
19 who is in the FTC's Bureau of Economics. Lou, are you
20 joined today by Haj?

21 MR. HADEISHI: Yes, I'm here. Thank you.

22 MR. DAVIS: That's Haj Hadeishi, another
23 economist in the FTC's Bureau of Economics. Also on the
24 line with me is Allyson Himelfarb, our outstanding
25 investigator, and I'll just take one more second to ask

1 whether we are joined by Chris Lewis?

2 MR. LEWIS: Yes, I'm here.

3 MR. DAVIS: Thank you, Chris. I think that is
4 everyone. Fantastic. Well, thank you all again for
5 joining us for a two-hour conference call to talk about
6 the federal CAN-SPAM Act.

7 As you know, in December 2003, Congress enacted
8 and the President signed the CAN-SPAM Act which, among
9 other things, directs the FTC to report on the
10 effectiveness and enforcement of that Act. The FTC's
11 report is due to Congress by the middle of December
12 2005, which would be basically on the two-year
13 anniversary of the passage of the Act.

14 The FTC has been gathering data since the
15 passage of the Act, and this interview with you all will
16 be transcribed for the record and will be part of the
17 record for the report. This interview is just one of
18 several ways the FTC is seeking information that would
19 be relevant for the report on the effectiveness and the
20 enforcement of the CAN-SPAM Act.

21 Because today's call is being transcribed for
22 the record by a court reporter, who is listening to the
23 call, it is very important that when you wish to speak
24 you begin by stating your name and your affiliation.
25 For example, this is Mike Davis with the FTC. If you

1 don't remember, one of us will probably ask you to
2 please stop and identify yourself, and the call would
3 proceed much more efficiently if you would just make a
4 note now to state your name when you began speaking.

5 Also, to be absolutely clear, your views
6 expressed today here will be transcribed for the record
7 and may be appended to the report to Congress or
8 otherwise made public, and we just wanted to make sure
9 that everyone is clear on that.

10 Are there any questions before we begin?

11 Great. Today's interview questions will cover
12 four general topics: First, marketplace development or
13 technological changes since the passage of the Act,
14 December of 2003, that may affect the practicality or
15 the effectiveness of the CAN-SPAM Act, and this could
16 include, but is not limited to, changes in filtering,
17 methods of authentication, the new or increasing use of
18 non traditional devices for receiving Email messages
19 such as hand-held devices and cell phones, et cetera.

20 Second, the extent to which the international
21 transmission of Email may affect the effectiveness of
22 the Act and any suggestions or changes. Third, ways in
23 which consumers, especially children, can be protected
24 from obscene and pornographic material, and I might
25 reference the FTC's April 2004 Brown Paper Wrapper rule

1 in that context, and finally, of course we would like to
2 walk through the provisions of the Act one by one and
3 discuss the effectiveness of each of those provisions of
4 the Act.

5 For each of these four main areas, I will ask a
6 series of questions, and if you have any information
7 responsive to any of the questions, please signal your
8 interest verbally, and when you're called on, please
9 state your name and organization, and then go ahead and
10 provide your answer or your comment.

11 I would also like to take one quick moment to
12 indicate that there are many talented and experienced
13 FTC staff persons working on this report. I happen to
14 me among the most junior of them. I've been an attorney
15 here for four years, and I've litigated a deceptive spam
16 case in Federal Court, but that was in May of 2003,
17 before the existence of the CAN-SPAM Act.

18 Occasionally during this call, I may ask a
19 relatively obvious question for clarification,
20 particularly if an acronym is used or if a technique or
21 term sounds unfamiliar to me, and I apologize in advance
22 for such questions, but they are intended to ensure a
23 clear record for even moderately sophisticated readers.

24 Let's begin with the first issue, whether there
25 are any marketplace developments or technological

1 changes since the passage of the Act in December of 2003
2 that may affect the practicality or the effectiveness of
3 the Act.

4 Perhaps specifically I could start off by asking
5 whether there are any new or increasingly used methods
6 for receiving Email by consumers such as cell phones,
7 hand-held Email devices, and if so, do those affect the
8 practicality or the effectiveness of the CAN-SPAM Act?

9 MR. LEVINE: This is John Levine. Would you
10 like me to start?

11 MR. DAVIS: Please, John.

12 MR. LEVINE: The answer to the summary is
13 certainly yes. People are increasingly using hand-held
14 devices like Blackberries, and to some extent they're
15 getting Email as short messages on their cell phone,
16 although that's less popular in the U.S.

17 I'm not sure that makes a whole lot of practical
18 difference for the enforcement of the Act because for
19 most purposes, Blackberry Emails is the same as Email
20 you would do in your PC, and the charging is not
21 particularly different. It's just for people that use
22 their Blackberries all the time, spam is intrusive to
23 them all the time.

24 MR. DAVIS: Thank you.

25 MR. LEWIS: This is Chris Lewis. There is some

1 differentiation of affect with people who are using
2 devices like RIM where the possibility of receiving
3 Email are much higher than in the normal case of events,
4 and there's probably a lot of people who are not using
5 such devices because they would be getting too much
6 spam.

7 MR. DAVIS: Thank you, Chris. This is Mike
8 Davis. Could you clarify, what is RIM?

9 MR. LEWIS: These are hand-held combination cell
10 phone, Internet devices.

11 MR. LEVINE: RIM is an acronym for research in
12 motion, which is a company that makes one of the most
13 commonest of these devices.

14 MR. DAVIS: Thank you.

15 MR. ADKINS: This is Steve Adkins, Word to the
16 Wise. I think one of the other major technological
17 changes is that the spam filters have become
18 significantly more aggressive because of the increasing
19 amount of spam, which increases the amount of legitimate
20 Email that gets blocked or thrown away, and it's making
21 Email less useful, certainly in a business context.

22 MR. DAVIS: So that would be a consequence of
23 filtering not only for say cell phones or hand-held
24 devices but just any type of user who receives Email.

25 MR. ADKINS: Exactly, all Email, and it's

1 getting more aggressive. More legitimate Email is being
2 thrown away, and that's causing Email to become less
3 useful in a communications medium.

4 MR. DAVIS: Thank you, Steve. I was planning on
5 moving into filtering next, although certainly I welcome
6 any comments on that in this context as well. Perhaps I
7 can ask whether in the context of wireless devices, are
8 there any concerns with regard to the ability to access
9 any opt-out link that might be contained in the Email?

10 MS. LIEB: This is Rebecca Lieb of the Clickz
11 Network. I was going to raise that concern, and I also
12 would like to expand on Chris Lewis's point about the
13 cost of receiving Email on certain wireless devices.
14 It's not necessarily limited to RIM devices, but
15 dependent upon somebody's cell phone plan, the cost of
16 receiving spam can become prohibitively Hi. Therefore,
17 consumers may not be opting for these higher cost plans
18 with Internet access on wireless devices because of the
19 real or potential cost of receiving spam.

20 MR. DAVIS: Thank you. Why don't we move on to
21 Email filtering, and let me ask whether there have been
22 changes to filtering that affect the practicality or
23 effectiveness of the Act, and I think Steve's comment
24 probably goes to this question.

25 MR. DELLA PENNA: This is Mike Della Penna,

For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555

1 Bigfoot Interactive. We did some research in February
2 of 2005, and we found a couple of interesting data
3 points. First, the use of anti-spam filtering from the
4 consumer's perspective, including challenge response
5 software, seems to be increasing. About 65 percent of
6 our consumers surveyed said that they are implementing
7 or using such software.

8 At the same time, that is being balanced with
9 very much an increase in consumers taking action to
10 increase legitimate senders to their address book, to
11 protect those communications and the delivery of those
12 communications, so we're seeing consumers taking efforts
13 to keep the bad stuff out; at the same time taking
14 initiative to assure delivery of wanted communications,
15 so consumers I think are becoming a lot more educated
16 and a lot more proactive in managing their inbox.

17 By the way, the add to address book stats that
18 we have is 56 percent said they always add a legitimate
19 or trusted sender to their address book, so that's the
20 kind of data we have seen most recently.

21 MR. COHEN: This is Jordan Cohen of Bigfoot
22 Interactive. I would just like to add on top of what
23 Mike just said. Clearly there's been improvements in
24 filtering, at least at the largest ISPs, which account
25 for the lion's share of consumers' accounts.

1 As many of us are aware, at the end of last
2 year, America OnLine announced the first breakthrough,
3 actual decline in spam that their members received, both
4 in terms of the volume being sent to them and also in
5 terms of the number of spam complaints that their
6 members were reporting, for the first time since 1999
7 and also in a dramatic way, and to further that point,
8 AOL was really one of the first ISPs, and pretty much
9 all of the major ISPs right now provide their users with
10 browser based spam feedback buttons, which have been
11 tremendously helpful in really providing, end-user
12 control.

13 Our studies, the Bigfoot Interactive Research
14 Study, also found that about 70 percent of consumers
15 correlate clicking the report spam button with receiving
16 less spam or not having to report spam in as great
17 frequency as they had previously.

18 MR. LEWIS: This is Chris Lewis. I should make
19 a remark about the AOL experience. AOL is such a large
20 organization that spammers treat them differently.
21 Where AOL is seeing a decrease in spam volumes and some
22 other ISPs are as well, that's largely because AOL and
23 many ISPs are getting so good at filtering that spammers
24 are less likely to spam them.

25 Other organization such as ourselves are still

1 seeing spam volumes increase.

2 MR. ADKINS: I would like to concur with that.
3 I'm seeing the overall trend upward.

4 MR. DAVIS: Excuse me, is this Steve?

5 MR. ADKINS: Yes, Steve Adkins, Word to the
6 Wise. The overall trend is upward, but particular
7 organizations which I'll say AOL, Hotmail and to a
8 lesser extent Earthlink are very much a special case and
9 are treated very differently by bulk mailers, both bulk
10 mailers and spammers, and so their experience of mail
11 volumes, mail legitimacy isn't necessarily
12 representative of the nest as a whole, and because of
13 that, it's certainly not representative of what's
14 happening in the business to business mail market.

15 MR. COHEN: This is Jordan Cohen from Bigfoot
16 Interactive again. We should add the caveat that we are
17 certainly talking about the largest consumer ISPs, and
18 just to give some perspective, us as a bulk sender, on
19 average, consumer marketing lists are composed of
20 anywhere between 60 and 80 percent within those largest
21 ISPs, so in terms of the consumer experience, that was
22 where our comments were directed to.

23 MR. CASTELLI: This is Eric Castelli of
24 LashBack. I can't help but interject the advent of
25 authentication, and then upcoming reputation systems

1 which should help track and identify the initial sender
2 of Email.

3 Additionally, LashBack is an organization, and I
4 think there's others coming, who's actually monitoring
5 unsubscribe compliance, so we have the ability to
6 finally track down and figure out who the good guys are
7 and the bad guys are when it comes to unsubscribe and
8 CAN-SPAM.

9 MR. DAVIS: Thank you, Eric. I was about to
10 move on to authentication, and that gives me a good
11 segue, but I would like to ask Mike and Jordan if those
12 studies they referenced are available on your web sites.

13 MR. DELLA PENNA: We can Email it to you. We
14 have submitted a copy of the study to Sana Coleman over
15 at the FTC.

16 MR. COHEN: We've also attached it in our
17 response to the NPRM.

18 MR. DAVIS: All right, thank you. I'm sure that
19 we do have that. At the end of this call, I would like
20 to give out my Email address for anyone who has any
21 suggestions for materials that we might want to make
22 sure that we include in our research. I'll give that
23 Email address right now. M, as in Mike Davis, D A V I S
24 @ftc.gov. Mdavis@ftc.gov, and if you don't mind sending
25 that to me as well as the fact that you sent it to Sana,

1 that would be very helpful to us.

2 Why don't we move on to authentication. What
3 change, if any, regarding authentication may be
4 affecting the practicality or effectiveness of the
5 CAN-SPAM Act?

6 MR. DELLA PENNA: Mike Della Penna, Bigfoot
7 Interactive. I think we're seeing some progress on the
8 authentication front certainly with the implementation
9 of Sender ID. There are, according to MSN Hotmail,
10 approximately one million plus domains who have already
11 published SPF records.

12 The first Email Authentication Implementation
13 Summit was held earlier this month, July 12, here in New
14 York City to encourage industry ranging from small
15 businesses to Fortune 2000 companies to implement
16 authentication standards, including some of the
17 cryptographic solutions and IP based solutions, so there
18 is, I think, a tremendous amount of progress being made
19 in educating the community as well as encouraging the
20 implementation of these standards.

21 Yahoo and Cisco have recently merged their
22 standard. Both that and Sender ID have been submitted
23 to the IETF for consideration, and we're seeing
24 certainly the bulk mailers comply with those standards
25 in a very big way.

1 Some initial data is also coming back as a
2 result of implementing those solutions, which have
3 benefited those who are up and running significantly as
4 it relates to reducing false positives and further
5 assuring delivery.

6 Microsoft I believe recently reported a 6
7 percent reduction in false positive incidents, so
8 overall (I'll keep my comments a little bit short here).
9 I think we're seeing great progress. The community is
10 coming together in a very big way, and education efforts
11 and more specifically instructional help is out there to
12 help large and small senders implement these solutions.

13 MR. ADKINS: Steve Adkins, Word to the Wise. I
14 would agree that there are two many widely discussed
15 authentication methods, SPF and Sender ID and DKIM from
16 Yahoo and Cisco. At the moment a lot of the energy is
17 being expended on SPF and Sender ID, which is a very
18 very poor authentication mechanism. It's useful
19 primarily for simplifying ISPs' white listing of senders
20 they do actively want to receive Emails from, but it's
21 actually fairly worthless as hard authentication in the
22 use for filtering out spam or recognizing forged Emails.

23 It's got wide deployment and a lot of mind
24 share, but it's actually quite ineffective and also can
25 cause an awful lot of false positive on legitimate

1 Email, particularly when mail forwarding is concerned.
2 If anything, I think it's going ahead to do more damage
3 to the Email network than less.

4 Yahoo DomainKeys and its success with DKIM, on
5 the other hand, don't have most of those drawbacks the.
6 Main issue with those they're more expensive to deploy
7 both for receivers and bulk senders. Despite that, I
8 think that it's going to have a big effect when they are
9 rolled out.

10 MR. DAVIS: Excuse me, Steve, just for the
11 benefit of Debbie, what is the acronym, DKIM?

12 MR. ADKINS: Honestly I don't recall. The
13 original acronym was DK for DomainKeys because it's a
14 public key based authentication based upon the domain of
15 the sender. DKIM is the successor of that.

16 MR. DAVIS: Thank you.

17 MR. COHEN: This is Jordan Cohen from Bigfoot
18 Interactive. That's DomainKeys Identified Mail.

19 MR. DAVIS: Great.

20 MR. DELLA PENNA: Mike Della Penna from Bigfoot
21 Interactive. I would just add that I think as publicly
22 stated by Microsoft themselves, Sender ID is just one
23 component in the fight against spam or the work that
24 they're doing to further identify legitimate senders
25 from the bad mail, so I think you have to look at it as

1 a component of a wider solution that includes
2 reputation. That includes legislation. That includes
3 all the things that industry has talked about, so
4 anything that can help the largest ISPs parse the mail
5 better can have a significant impact on legitimate
6 senders and reducing spam.

7 The other important point is -- I think
8 certainly all technologies are going to have drawbacks,
9 and this is an evolution, and we're building a
10 foundation from which to build upon, so things like the
11 forward problem have been widely recognized by Microsoft
12 as a drawback, but they are a step in the right
13 direction, and I think industry is pleased with the
14 progress that is being made.

15 MR. LEVINE: This is John Levine. I would have
16 to concur with Steve Adkins' remarks. Although there's
17 an been enormous push for Sender ID, I only see it for
18 white listing big sorts, big senders, which is not
19 useless but it's far from a complete solution to the
20 spam problem, and I'm even aware of some ISPs who have
21 withdrawn their SPF records because they're causing more
22 trouble than they're worth, and the IETF basically
23 rejected both SPF and Sender ID and designated them as
24 experiments and are done with them.

25 DKIM, on the other hand, is looking very

1 promising. The IETF is meeting in a couple weeks in
2 Paris, and it looks very likely that there will actually
3 be a process set there which will indeed turn them into
4 an IETF standard, which will certainly help their
5 adoption.

6 I think it's also worth pointing out for all
7 these things that no authentication scheme is useful
8 without some sort of reputation system. People
9 consistently report that if you look at the mail that
10 passes SPF or Sender ID, the majority of it is spam
11 because spammers can tag their mail just like anybody
12 else.

13 MR. DAVIS: Let me ask a catchall question. Are
14 there any other marketplace developments or
15 technological changes that you believe might affect the
16 practicality or effectiveness of the Act, and we can
17 look at this sort of in retrospect, looking back over
18 the last 18 months or so, or if you feel like your
19 crystal ball is sufficiently polished, if you can look
20 forward into the next six months to a year and identify
21 any marketplace developments or technological changes
22 that are likely to affect the practicality or
23 effectiveness of the Act.

24 MS. LIEB: This is Rebecca Lieb from the Clickz
25 Network. I think it should be mentioned that while this

1 is tangential to Email, it is my belief, and I'm seeing
2 a lot of evidence that RSS technology is going to have a
3 big impact on the volume of Email now and increasingly
4 in the future.

5 MR. DAVIS: Thank you, Rebecca. What is that
6 acronym again, please?

7 MS. LIEB: RSS is an acronym for Rich Side
8 Syndication or Real Simple Syndication. It is the
9 technology that delivers headlines, news feeds, blog
10 feeds, and basically any type of enabled information
11 online into an RSS reader, into your My Yahoo Page.
12 Today Google announced that they were also going to
13 adapt this technology.

14 It's being very broadly adopted by the large
15 portals, including AOL, and it is enabling consumers to
16 unsubscribe from Email newsletters primarily, but
17 increasingly product updates, notifications from
18 businesses they frequent, and it is enabling people to
19 disengage from Email and to receive their information in
20 another format.

21 I raise this because I think it's going to have
22 an impact, not so much on the Act, but the necessity of
23 sending and receiving Email.

24 MR. DAVIS: Thank you.

25 MR. LEVINE: This is John Levine again. I

1 concur with that. I think we will see a lot of what is
2 now sent as bulk Email sent as RSS instead, and since
3 the recipient preselects what RSS he's going to get,
4 it's extremely resistant to spam.

5 It's also worth mentioning the IETF has a
6 project called ATOM, A T O M, which doesn't stand for
7 anything, which is basically a codification and
8 standardization of RSS. I happened to have dinner with
9 the chair of the ATOM Project Sunday night, and he said
10 it's almost done so I think we're going to be seeing a
11 lot more of that.

12 On the other hand, RSS does not replace person
13 to person Email. It only replaces broadcast Email.

14 MR. LEWIS: This is Chris Lewis. As John said,
15 and I wanted to amplify, was it replaces the bulk Email
16 so you got to choose what advertisements you get, but it
17 does not mean that you're not getting Email anymore, so
18 in order for RSS to make a significant impact upon
19 Email, people will at least have to abandon one set of
20 Email addresses and go to another that they only
21 advertise to their closest friends and use RSS for
22 anything else, and I don't really see that happening.

23 MR. DELLA PENNA: Mike Della Penna from Bigfoot
24 Interactive. I think in addition to the comments that
25 have been made, many of the leading analysts, including

1 David Daniels at Jupiter Research, have covered RSS, and
2 basically believe it is a supplement to Email, and its
3 adoption is several years out, until we reach critical
4 mass, so as far as the immediate impact, very little.
5 Long-term perhaps, but it is very much in its early
6 stages and does require users to download readers and
7 take action.

8 So its adoption, like all technology that
9 requires downloading, will be slower than Email, so I
10 think we have to put it in perspective as it relate to
11 the immediate impact on CAN-SPAM.

12 MR. COHEN: Jordan Cohen, Bigfoot Interactive.
13 Just bringing it back to Email from RSS, Email is here
14 to stay, and definitely we're optimistic about how
15 things are going to unfold in the next couple of months.
16 As noted, already there have been marked improvements
17 over the last years, but I think as John Levine
18 mentioned earlier, authentication solutions alone aren't
19 enough, and we do anticipate that reputation and
20 accreditation systems will continue to proliferate.

21 As we know at MSN Hotmail, they signed an
22 agreement with Bonded Sender a year ago, and they're
23 planning to implement also Habeas later this year.
24 We're anticipating that several other big ISPs will
25 announce similar types of agreements with third-party

1 accreditation and reputation vendors before the year
2 ends.

3 Those are going to be very positive in terms of
4 further reducing the issue of false positives, making
5 the medium much more reliable for legitimate, permission
6 based marketers, and by that same token, we anticipate
7 that that would make it easier for ISPs to further
8 distinguish and protect their users from spam.

9 MR. ADKINS: Steve Adkins, Word to the Wise.
10 There has been one technological change that has been
11 directly driven by the CAN-SPAM Act. A number of the
12 out-sourced bulk Emailers and bulk spammers who spam for
13 other people have integrated into their automatic
14 systems codes that makes every Email they send out
15 CAN-SPAM compliant by putting in contact information and
16 things like that.

17 That doesn't actually make any change to the
18 fact that what they're sending is spam and is still
19 unwanted, but it means that the overhead of complying
20 with the CAN-SPAM Act for the spam their customers send
21 out is effectively zero.

22 The main effect that's had is to allow those
23 bulk out-source spammers to represent themselves to the
24 business community as doing everything right, being
25 quite legitimate, and it's no additional effort for you

1 as a customer to comply with these regulations, and what
2 we're doing is completely legal and acceptable. That's
3 being done at all out-sourced bulk mailers, both
4 legitimate, illegitimate and the outright spammers.

5 MR. LEWIS: This is Chris Lewis of Nortel. It
6 basically boils down to the fact that CAN-SPAM didn't
7 outlaw spam. It just said, If you spam, you must follow
8 the following rules, and spammers are very good at
9 following such rules and coming up with new techniques
10 to make them easier to do.

11 MR. DAVIS: All right. Thank you. Let me ask a
12 question about opting out and whether anyone has any
13 information or has maybe even seen any studies that
14 would validate or confirm a concern that has been
15 expressed that by using opt out, you might subject
16 yourself to the negative consequences that it has.

17 MS. LIEB: Absolutely.

18 MR. DAVIS: That is Rebecca?

19 MS. LIEB: Rebecca Lieb, Clickz Network. I'm
20 increasingly seeing Emailers who, when you opt out, lob
21 your Email address over to other domains, so you
22 continue to get spam, although it appears that you are
23 opted out from the domain or the sender that you opted
24 out from. What the relationship is between who you were
25 getting Email from and who you are getting Email from is

1 very mirky, but it certainly existed.

2 MR. CASTELLI: This is Eric Castelli from
3 LashBack. Our company is primarily focused on
4 unsubscribed and not only what firms are honoring
5 unsubscribe requests, but also which ones are abusing
6 them.

7 The way we identify that is we programatically
8 submit a probe or fake Email address to any unsubscribe
9 mechanism we encounter, and then we wait to see if spam
10 is sent to that probe Email address. If it is, it
11 basically identifies the fact that the suppression list
12 of the organization has been shared with another party,
13 either legally or illegal, and that third-party sends
14 Email to it.

15 Currently we track about 120,000 different
16 unsubscribe mechanisms. Of those, approximately 8,500
17 are falling into that category; thereby basically 8,500
18 or 8.5 percent of the unsubscribe links out there, if
19 you submit your Email address, you're basically going to
20 get more spam. So it is a large problem in the
21 industry.

22 MR. DELLA PENNA: Mike Della Penna from Bigfoot
23 Interactive. I think the trust in the unsubscribed
24 mechanism from the consumer perspective is no longer
25 there. In a study that we conducted, about 58 percent

1 of consumers believe that unsubscribing from an unwanted
2 Email has resulted in receiving additional Email.

3 I think because of a lot of the efforts and
4 education, even from some of the leading ISPs, that tell
5 consumers not to trust the unsubscribe mechanism,
6 consumers are hesitant of using that mechanism as a
7 result of that. So I think we're seeing a lot more,
8 from our perspective, of consumers replying to Emails to
9 unsubscribe as opposed to using the link. That's
10 definite trend.

11 MR. ADKINS: Steve Adkins, Word to the Wise.
12 The significant fraction of spam out there where the
13 main goal of the person or the code sending the spam is
14 to get the end user to click on a link, any link,
15 particularly mail born viruses. The use of a web link
16 within the mail to unsubscribe means that even if one of
17 these tries to unsubscribe, what they've really done is
18 they have done what the senders mail wanted them to do,
19 which is go to a particular web site, often which will
20 try and compromise their machine.

21 That's not something that I've seen done often,
22 but I have seen it a few times, and the trend seems to
23 be increasing, which might be another reason why links
24 within Email, despite their convenience, consumers are
25 beginning to realize that the link within the Email is

1 not always the safest place to unsubscribe from the
2 list, even lists they've signed up for intentionally.

3 MR. LEWIS: Chris Lewis from Nortel. I also am
4 heavily involved in our anti-virus infrastructure, and
5 we tell our users not to click on any links in Email
6 they weren't expecting because so much of the viruses,
7 whether they're phishing attempts -- or sorry, start
8 that again.

9 So many of the Emails that people are getting
10 are specifically trying to infect you, via a link in the
11 Email, whether it be a phish or whether it be a better
12 human engineering in viruses that our users are told
13 explicit, Do not click on any links on Email you didn't
14 expect. Don't even try to peak at them to find out what
15 it is because the viruses are becoming such a problem
16 that it's not longer safe ever.

17 MS. LIEB: Rebecca Lieb, the Clickz Network. I
18 would like to add to that even when unsubscribed links
19 aren't explicitly there to give you a virus, I've seen
20 on several occasions links that spun so many pop-up
21 windows and web-based advertisements in your browser
22 that the only way to get rid of them is literally shut
23 down your entire computer, so it turns into browser spam
24 when you attempt to unsubscribe from an Email spam.

25 MR. LEWIS: This is Chris Lewis again. We

1 include that in a general ad in viruses or we include
2 Adware and Spyware as viruses. The effect is exactly
3 identical, to infect your machine with stuff you didn't
4 want.

5 MR. DAVIS: Thank you. So there's some strong
6 feeling on that topic. If anyone has anything published
7 that they would like to share or has seen anything
8 published that they could either make some kind of
9 reference to it or send me a copy of an article, we
10 would really appreciate that. We would like to look at
11 all the information about those negative consequences.

12 Moving on, there has been a recent study by the
13 Pew Organization that found that while the volume of
14 Email seems to have increased since the passage of the
15 CAN-SPAM Act, the frustration of recipients has
16 decreased. What, if anything, do you make of that
17 finding?

18 MR. ADKINS: Steve Adkins, Word to the Wise. I
19 think this is increasingly aggressive spam filters are
20 getting better and better about keeping unwanted mail
21 out of the people's mailboxes, which means despite the
22 increase in volume, the amounts actually making it to
23 the end mail box is probably going down in many places.
24 That decreases the frustration with spam, which is what
25 the survey was looking at.

1 The converse of that is more and more legitimate
2 is being blocked or discarded, and so there is a certain
3 level of frustration with Email being unreliable, but
4 that won't be included in the survey about whether spam
5 is causing frustration.

6 MR. LEWIS: This is Chris Lewis of Nortel. I'm
7 involved with the Federal Anti-Spam Task Force in
8 Canada, as is John Levine as well. The Task Force has
9 completed, except for one effort going along, with
10 statistics in Canada as part of an OECD effort. We are
11 going to be coming up with a set of unified statistics
12 that are comparable across the world about the influence
13 of spam, and it's clear that we need to measure two
14 distinct things.

15 One of them is we have to measure the volume of
16 the spam from a technical bandwidth operational
17 administrative perspective, and the other aspect is is
18 that we have to measure a user perception issue.

19 When you consider Internet as being a major
20 economic driving force, the actual numeric volumes mean
21 nothing. It's user perception and how they embrace the
22 Internet and exercise economic activity over the
23 Internet which is of importance to industry and
24 government worldwide, so the OECD is going to be
25 measuring both.

1 I believe that France is currently starting up a
2 survey of their -- of the French population on those two
3 very issues.

4 MR. DELLA PENNA: Mike Della Penna, Bigfoot
5 Interactive. I think we're seeing two things happening.
6 Number one is consumers in the research we conducted
7 noted a decrease in the volume of spam they're
8 receiving. In addition I think consumers are viewing
9 any Email that is irrelevant as spam, and there is a
10 trend that we're seeing towards more relevant,
11 contextually targeted communications, and consumers when
12 asked whether or not the relevance of Email has
13 increased over the past year, the majority said yes.

14 So I think the legitimate marketers are very
15 focused at evolving their communications around
16 consumer's needs more aggressively than they have in the
17 past, which has resulted into an increased acceptance of
18 that Email. We can forward that research again to you.

19 MR. DAVIS: Thank you. Okay. Well, still on
20 the first theme of marketplace and technological
21 developments, why don't we talk a bit about zombie
22 drones, which are innocent user's machines that are
23 highjacked by spammers through some kind insecure
24 connection.

25 Has the use by spammers of zombie PCs or

1 networks had an impact on the effectiveness of the
2 CAN-SPAM Act, and are spammers able to basically comply
3 with the Act but use new technology to customize
4 individual Emails or campaigns and thus avoid detection
5 as a source of large volumes of spam?

6 MR. LEWIS: This is Chris Lewis of Nortel. The
7 answer is definitely. The use of open proxy zombies is
8 now up to the 80 percent level for sending spam; in
9 other words, 80 percent of all spam is sent that way.

10 The numbers that are being used, that are being
11 detected and used in this way are not decreasing. Just
12 ourselves our detecting on the order of 250 to 300,000
13 new ones a day. The CAN-SPAM Act does not seem to have
14 had any affect with these because many of these entities
15 who are running the zombie networks are well known to
16 us.

17 The zombie networks are ipso facto violations of
18 some of the -- I'm about to use Canadian terminology,
19 indictable offenses under the CAN-SPAM Act, but the
20 vendors are still in operation, and they have not been
21 negatively affected at all, and if anything, their
22 volumes are much higher than they were.

23 MS. LIEB: This is Rebecca Lieb of the Clickz
24 Network, and I'm going to go out on a bit of limb with
25 these comments. It's always seemed to me that a

1 critical element in this problem is that the earlier
2 Windows Operating Systems were shipped default as open
3 relays, and consumers have not been educated to shut
4 those open relays. It's an easy configuration. I'm
5 wondering if some measures could be taken directly with
6 Microsoft that would go far to fix that problem.

7 MR. LEWIS: This is Chris Lewis again. The
8 software that's being used to do this and the techniques
9 that are being used to do this are not really what you
10 would call things that the Microsoft Operating System
11 can normally do, so it's not matter of an open relay
12 being left or being turned on by default.

13 That used to be an issue, but that has not been
14 an issue for many years. The issues we have now, and to
15 be out and out security folds in Windows, and one or two
16 other instances that are being exploited by things that
17 are exploiting. It is not a specific whole as opposed
18 to a default security or default setting.

19 The things that are being used to infest a
20 machine with a zombie or an open proxy are not things
21 you have to turn down. They are things you need
22 patched, so much as we like to bash the users in some
23 cases about running sloppy machines and not being
24 educated well enough, we are past the point where
25 education would make a great deal of difference, other

1 than you shouldn't have a fire wall. You should have
2 this. You should have that, but the software itself is
3 flawed, and in many cases it's the software itself is
4 the problem rather than the users.

5 On the other hand, many of the biggest problems
6 we've had in terms of viruses likes Nets Key and Bagle
7 have required a human being to actually click on the
8 link and do something. Bagle was typically a good
9 example where you would get this Email, and it has this
10 password as a picture, and you have to type in the
11 password, and it physically says, Here's your Email,
12 please click on this link and type in this password, and
13 a surprising number of people would do that.

14 MR. ADKINS: Steve Adkins, Word to the Wise.
15 End users are being trained to do that by challenge
16 response mail filtering systems, which are part of the
17 problem rather than part of the solution.

18 MR. SILVERVIN: This is Lou Silvervin. Just a
19 clarifying question on the zombie drones. If everybody
20 has firewalls, would they be prevented.

21 MR. ADKINS: Steve Adkins, Word to the Wise.
22 No, absolutely no. A firewall or a consumer net filter
23 is a good thing to protect you from the nets at large,
24 but the vast majority of the Email borne virus that are
25 being sent out propagate via the user's mail reader.

1 MR. SILVERSIN: I'm sorry, that's not the
2 question I'm asking. The question I'm asking is: In
3 order to propagate these Emails, they've taken over
4 somebody via and made them into a zombie drone.

5 MR. ADKINS: If you'll let me finish.

6 MR. SILVERSIN: No, no, no. My question is:
7 Would that take over have been prevented if that user
8 had a firewall?

9 MR. ADKINS: If you'll let me finish. The
10 firewall is a good thing to have, but most of the Email
11 viruses that are used to compromise these machines come
12 in via Email. They infect the machine via the use of
13 mail clients, so Outlook, Outlook Express is typically
14 vulnerable to this, but other mail clients are too.

15 Once they've compromised that machine, they do
16 several things. One thing they do is they send out more
17 copies of themselves to compromise other machines. The
18 other thing they do is they open up back channels
19 through various routes, so the person who sends out the
20 virus in the first place can identify that this machine
21 is compromised, know that it's ready for use, and when
22 they need it, they can use it.

23 So the mail borne viruses, these days certainly,
24 the primary function of them is to compromise machines
25 for future use, and the firewall will not protect you

1 against that at all, but when the machine is compromised
2 the, next stage that's very commonly done is those bot
3 necks, they're not actually intended to be sold to
4 spammers outright, but they tend to be rented out to
5 spammers to send spam or the back channel is known and
6 they're comprised by other spammers to send spam.

7 At that point, some wire walls used to be able
8 to protect the net at large by blocking the outgoing
9 mail from the infected machine. It didn't protect that
10 machine but it protected the rest of the net. Less and
11 less is out being useful because the virus rises and the
12 people compromising those machines to send spam worked
13 around it and are now trying to send stuff out to the
14 ISPs smart host, to a significant extent at which point
15 the traffic is, apart from the volume, indistinguishable
16 from normal traffic from that user.

17 MR. SILVERSIN: This is Lou Silversin again.
18 Just a quick follow-up, if I might. Back to the
19 original source of the infection, so it comes in through
20 the mail, and it's a mail borne virus. Presumably if
21 the user doesn't click on or doesn't open the virus, he
22 or she would be protected?

23 MR. ADKINS: No.

24 MR. SILVERSIN: If they're not reading the
25 message.

1 MR. ADKINS: It depends on the mail reader.
2 Certainly for quite a long time Outlook and Outlook
3 Express had what was called a preview page. They still
4 do. It was possible for the machine to become infected
5 simply by receiving the Email and the user selecting it
6 in the list of mails. They wouldn't need to open it or
7 they wouldn't need to click on anything. It would just
8 affect the machine immediately.

9 Some of those security issues have been fixed so
10 it's more likely these days they would need to click on
11 something, but that's just a gradual evolution of
12 security. I'm sure there will be another security
13 compromise soon that again will not require anybody to
14 click on it.

15 MR. SILVERSIN: A virus protection does not work
16 on these?

17 MR. ADKINS: Virus protection is the software
18 you would hope that would block these, but for a number
19 of reasons, it's not as effective as you would want it
20 to be, not least because these things propagate very
21 rapidly, and they can propagate across the world in
22 significantly less time than most people update their
23 virus filter heavily.

24 MR. LEWIS: This is Chris Lewis at Nortel. We
25 are seeing a significant number of new viruses per day.

1 We're at times seeing five or ten viruses that we report
2 to our anti-virus vendors that they have not seen
3 before, so when you're dealing with ten new varieties a
4 day that a single, all be it relatively large
5 corporation, sees, the AB vendors haven't seen before,
6 you can appreciate that anti-virus and firewall products
7 are lagging by significant margins.

8 MR. SILVERSIN: Okay.

9 MR. LEWIS: The other things that should be
10 pointed out is that most of the big anti-virus
11 industries, in the last year or so, have been things
12 that required to have users do something, but most of
13 these viruses continue to use the old techniques that
14 caused them to be automatically imposed when you hit
15 preview.

16 They're still using the Melissa tricks, Klez,
17 that caused automatic indication just like previewing or
18 selecting. They're still using those techniques. There
19 are still some people that get infected by it.

20 The viruses tend not to abandon techniques.
21 They just tend to bundle yet more that they can affect
22 or propagate.

23 MR. DAVIS: Well, thank you. That would
24 conclude our first theme, the marketplace and
25 technological development.

1 I would like to let everyone know that we've
2 been joined by our colleague here at the FTC, Katie
3 Harrington-McBride. You may hear her voice, and she
4 knows. She's been on these calls before, she knows that
5 she will say her first name for Debbie's benefit and
6 everyone else's if she has a question, but she may jump
7 in from time to time. I will just continue to lead us
8 through the rest of this conference call.

9 Our next topic is how to address commercial
10 Email that originates in or is transmitted through or to
11 facilities or computers in other nations. Congress
12 wants the FTC's report to include analysis and
13 recommendations on this, including initiatives or policy
14 positions that the United States could pursue.

15 So first to what extent does Email received in
16 the United States originate in or get transmitted
17 through other countries and are methods for identifying
18 origins of Email adequate?

19 MR. LEWIS: This is Chris Lewis of Nortel. I'm
20 sure Steve and John would agree with me if I were to say
21 that probably more than 50 percent of all the spam that
22 we are getting are coming from outside of the United
23 States, North America and Europe.

24 However, for the most part, these are on the
25 behest of or fulfilling business interests of people who

1 are usually in the States. From our perspective
2 probably in excess of 90 percent of the people who are
3 responsible for sending the spam are American, but the
4 actual source of the Email and where the web sites are
5 is mostly in China, Korea or Brazil and a few places
6 like that.

7 So in a sense, the CAN-SPAM Act has had
8 relatively little effect, other than getting the
9 originators of this material to out-source their actual
10 operation.

11 MR. DAVIS: Does anyone think that the amount of
12 Email that is originating or transmitted through other
13 countries, is it changing since the passage of the
14 CAN-SPAM Act?

15 MR. ADKINS: Steve Adkins, Word to the Wise. I
16 don't believe it is much because honestly I don't
17 believe that either the legitimate bulk Emailers or the
18 spammers pay much attention to the CAN-SPAM Act other
19 than lip service. I don't believe it's changed anything
20 operationally. I think what's driving on shore or
21 offshore is simply a matter of economics.

22 Is it cheaper to get a fairly secure
23 connection where you won't be kicked off in the U.S., or
24 is it cheaper to buy one in Russia or China these days,
25 trade that off with mail from China more likely to be

1 flittered than say from mail from Florida. So I think
2 that there will be a change as the months go on between
3 where the spam is being sent primarily from offshore or
4 primarily from onshore.

5 There's always going to be a lot of internal
6 spam. There's going to be a lot of external spam. The
7 exact balance is simply going to be driven by the
8 market.

9 MR. LEVINE: This is John Levine. It's also
10 going to be affected somewhat by policies in various
11 countries. I mean, China had a completely lax attitude
12 towards spam until very recently. When I was at the ITU
13 Security Conference earlier this month, I was surprised
14 to see that China finally realizes that hosting American
15 spammers is no longer in China's interest, and they're
16 in the process of pushing them off, so my guess is we're
17 going to be seeing more of it appearing in Russia and
18 Eastern Europe where the enforcement is still pretty
19 bad.

20 MR. LEWIS: Chris Lewis. I'm looking at some
21 metrics that show where the preponderance of our spam is
22 coming from over the last year and a half or so, and the
23 single biggest source of spam sent to us for the last
24 several years has been primarily the United States.
25 There has been a short, a month or two -- the last month

1 or two Korea popped up above it, but we do see Korea has
2 been making some strides recently and China has been
3 making some strides where the volumes tend to be fairly
4 static.

5 MR. DAVIS: I'm wondering if there are any
6 suggestions on any ways to improve the methods that
7 exist for identifying the origin of Email.

8 MR. LEWIS: This is Chris Lewis. For the most
9 part anyone who knows how to take a look at headers can
10 figure out where the Email has been sent from. The
11 trick then becomes who sent it and on whose behalf was
12 it sent, so I mean, we can tell with virtual 100 percent
13 certainty where every single piece of Email that hits us
14 was sent from in terms of the machine that sent it to
15 us.

16 The question then becomes, How do we interpret
17 the content of the message to find out who was
18 responsible for it. That's hard, and that's not
19 something that the technology will help us with.

20 Spamhaus being a good example of an organization
21 who spends its time trying to track who is sending these
22 things, who is responsible for them, and they're pretty
23 good at identifying it, but it requires a great deal of
24 legwork and noticing similarities from one spam to
25 another and tracking things back through Who Is database

1 and so.

2 MR. ADKINS: Steve Adkins, Word to the Wise.
3 Can you clarify the original question? Are you talking
4 about the CAN-SPAM requirements for including say the
5 physical address of where the mail was sent from?

6 MR. DAVIS: No, I don't actually have that
7 physical postal address requirement in mind. I was just
8 thinking about the technical ways that you might use to
9 trace the origin of Email and whether there were any
10 suggestions on how to improve that, not an explicit
11 issue addressed by the Act.

12 MS. HARRINGTON-MCBRIDE: This is Katie. I'm
13 sorry to step in. I just thought maybe for further
14 clarification, one of the things that we've seen in
15 tracking the literature on spam and what's been
16 happening in the last 19 or so months is that you see
17 different figures reporting the origin of the spam.
18 It's not fairly widely different, and we're trying to
19 figure out whether there are different methodologies and
20 whether there's a preferred methodology for assessing
21 the origin.

22 MR. ADKINS: Steve Adkins, Word to the Wise.
23 One thing is is that the origin is very ill defined in
24 some respects because as Chris said, 80 percent of mail
25 is sent through compromised machines. Different places

1 on measuring different things, some of them are
2 measuring where the web site happens to be hosted. Some
3 of them are measuring the language the spam is sent in.
4 Some of them are measuring the compromised machines that
5 were used to send it. Some of them are measuring the
6 spammers they believe were responsible for it, where
7 they live, and all of those things are measuring
8 different things.

9 Also different people get different spam.
10 Different mailboxes get wildly different spam. Somebody
11 on AOL will often get very different spam from somebody
12 on Earthlink. I have multiple mailboxes that deliver to
13 me on the same machine. The type of spam they sent
14 though is drastically different, so depending on which
15 spam I have on that particular Email address, it can
16 vary widely, not only the content and the type of spam,
17 but it's because it's different spammers where it's sent
18 from.

19 So a lot of the commercial surveys done are done
20 by analyzing a small number of probe accounts, and
21 depending on just the way the dice falls, which spammers
22 get ahold of those particular probe accounts, they may
23 see drastically different data. I think the only way to
24 get a good global overview is the work that's coming out
25 to the big ISPs who have huge numbers of Email

1 addresses, and so they'll be more consistency.

2 Conversely of course, AOL, Hotmail, Earthlink
3 are all special cases, and there are spammers who
4 concentrate solely on the big ISPs so they'll see the
5 data spewed in yet another direction.

6 MR. LEWIS: This is Chris Lewis of Nortel. We
7 have a fairly representative sample. On the other hand
8 we have one user who is getting 1,000 spams a day, and
9 yet 50 percent of our employees aren't getting any. So
10 it's just a matter of luck of the draw. It's what each
11 user sees is intensely variable from day-to-day.

12 MR. DAVIS: Okay. Thank you. So as many of you
13 may know, the FTC works closely with various
14 international organizations to monitor Email trends and
15 laws. Are there any thoughts about these initiatives or
16 other initiatives that could be undertaken? For
17 example, could the use of immediate economic restraints
18 against spammers in other countries prove effective, and
19 how could this be implemented?

20 MR. COHEN: This is Jordan Cohen from Bigfoot
21 Interactive. I would just say that Bigfoot Interactive
22 is definitely supportive of education on all fronts, and
23 we're definitely supportive of FTC efforts to go over
24 and educate other foreign governments and industries
25 about the problem, and definitely one of the biggest

1 important areas in this respect is things like
2 explaining to other countries how to secure your server,
3 that sort of thing, so we applaud those efforts.

4 We should also note that industry is moving
5 along with education on its own as well. The Messaging
6 Anti-Abuse Working Group, which we're a part of,
7 actually held their first international general meeting
8 over the summer in June in Dusseldorf, in Germany, and
9 one of the biggest things that MAAWG promotes, in
10 addition to standards and education, et cetera, is the
11 concept of self-containment, basically hitting the point
12 of what you were getting at earlier about open proxies,
13 open relays, and basically that every ISP, big and
14 small, has a responsibility to monitor its traffic on
15 its own network, so we think that continued education
16 efforts, both government and industry self-regulatory
17 efforts, will be critical.

18 MS. LIEB: This is Rebecca Lieb from the Clickz
19 Network. This is more of a macro observation, but based
20 on some of the comments that were raised earlier about
21 language and the real or perceived notion that most spam
22 is American in origination, the bulk of the spam in the
23 world is in the English language because the English
24 language is an extremely widely spoken language, and if
25 you're going for volume rather than quality, it's

1 unlikely you would be sending spam in Korean or in
2 Portuguese.

3 There's a very strong perception I think,
4 particularly in Europe, that it's the Americans who are
5 behind spam. I think the reality is that perception may
6 fluctuate, but the English language I believe is a
7 tremendous factor in this, and I would like to see the
8 United States at the forefront of efforts that will
9 salvage the reputation of businesses and the ethics of
10 doing business with American companies with these
11 companies afoot.

12 MR. LEVINE: This is John Levine. I'm a little
13 vague on what the original question was. My impression
14 was you were asking whether if you could arrange to shut
15 down spammers in other countries more quickly, that that
16 would help. Is that approximately it?

17 MR. DAVIS: Yes.

18 MR. LEVINE: Well, the answer in that case is,
19 yes, of course it would. I think in general the faster
20 you can shut down any spammer, the more effective it
21 will be because it will narrow the window in which they
22 can collect money from the suckers.

23 On the other hand, I think we're all aware of
24 just how hard it is to do any sort of legal process
25 internationally.

1 MR. LEWIS: This is Chris Lewis of Nortel.
2 Someone might answer this a little bit snarkely and say,
3 Well, it's a little hard for Americans to do this if
4 they're so bad at shutting their own native spammers
5 down.

6 MR. ADKINS: Steve Adkins, Word to the Wise. I
7 would have to agree. U.S. spammers operate for years
8 and years on end pretty much uninterrupted. They're
9 even spamming from particular ISPs for months to years
10 on end essentially uninterrupted, so you're not really
11 saying anything operational problems caused by pretty
12 much anybody.

13 The only thing that really impacts that business
14 badly is spam filters at the large ISPs. Given there is
15 pretty much or nothing to interfere with the moderately
16 careful spammer in the U.S. , I think speculating about
17 how it would be better if we could enforce overseas is
18 really a bit premature.

19 MR. LEVINE: In other words, clean up your own
20 house first.

21 MR. ADKINS: Steve Adkins, Word to the Wise
22 again. Not so much clean up your own house first as
23 most of the spam, a lot of spam that's being sent in the
24 U.S. isn't illegal. The only enforcement against it is
25 whether the ISPs providing them with connectivity want

1 to shut them down or not.

2 A lot of the spam that is being sent via
3 arguably a legal means, compromised machines and stuff
4 alike, it's very difficult to enforce against, and again
5 virtually impossible to track back to the original
6 sender, even if you follow the money. And once you've
7 done that, getting a useful legal case against them is
8 going to be difficult, so it's not so much the
9 difference between domestic and overseas enforcement as
10 whether there can be effective enforcement under the
11 current legal system.

12 MR. DAVIS: I'm sorry, it seems as though
13 someone's computer might be making some sounds. I'm not
14 sure if anyone out there has the ability to perhaps turn
15 down their speaker, but that might help a little bit
16 with the call.

17 Let me ask one more question in this area, and
18 that would be to what extent would any stricter
19 standards for domain registrars aid in addressing the
20 spam problem?

21 MR. LEWIS: This is Chris Lewis of Nortel. We
22 are seeing a number of spammers who generate very large
23 numbers of domains on very short intervals for a day and
24 then get rid of them. We're all seeing registrars who
25 are hiding behind or sorry, we're seeing spammers who

1 are hiding behind registrars who do not publish any
2 usable contact information.

3 Obviously there are legitimate reasons for
4 trying to protect our own private information. Canada's
5 registrar is struggling with that now with the privacy
6 legislation being enacted here, implying that our
7 internet publishers can't publish as much as they could
8 before.

9 However, the fact that the domains can be
10 registered quickly and in large numbers and largely
11 anonymously is a benefit to spammers, and it helps them
12 get passed filters. It's difficult to say what can be
13 done to assist this situation other than perhaps impose
14 a duty upon registrars to deal probably with the
15 problem.

16 MR. ADKINS: Steve Adkins, Word to the Wise.
17 It's very, very easy for someone to register a domain
18 name and give fake contact information. That's what a
19 lot of people do for various reasons to send spam out.
20 I don't see any way that the domain registrars could
21 really reduce that without drastic operational overhead
22 on their part. That would involve putting up the price
23 of registering domain names significantly.

24 Putting up the price of registering a domain
25 name significantly would be disincentive, but the value

1 of a throw away name to a spammer is drastically
2 higher than the value of a domain name registered for
3 real use for personal use.

4 So I think that anything that could be done that
5 would dissuade spammers from registering domains could
6 have a very bad effect on widespread public interaction
7 in the Internet, widespread publishing of their own
8 information, and I think the damage that would cause
9 would far outweigh the minor inconvenience to spammers
10 to make it more difficult to register a domain.

11 MR. LEVINE: This is John Levine. I'm on the At
12 Large Advisory Committee to ICANN, the organization that
13 oversees Internet domains, and they've been wrestling
14 with the issue of false domain information for quite a
15 long time, and at their meeting in Luxembourg a couple
16 of weeks ago, they wrestled with it again, and I don't
17 see them coming into any usual conclusion.

18 In theory, a domain with false information is
19 invalid. In practice, they don't have any opinion for
20 enforcement scheme, and since registrars are all over
21 the world, even if you enforce something on American
22 registrars, it is easy and common to register domains
23 through registrars in Europe and Asia, and so although
24 this is something that would be nice to fix, I think in
25 practice unless we can get a whole lot of other

1 countries to buy into it, nothing is going to happen.

2 MR. DAVIS: Well, thank you all. That would
3 conclude the questions that we have about the origin of
4 spam from overseas.

5 Our third issue relates to obscenity and
6 pornographic content that is contained in spam, and
7 Congress is interested in protecting consumers,
8 including children, from the receipt and viewing of such
9 pornographic or obscene Email message, so first let me
10 ask how effective do you think the sexually explicit
11 labeling rule that the FTC promulgated in April of 2004
12 pursuant to the CAN-SPAM Act has been in protecting
13 consumers, including children, from receiving and
14 viewing obscene or pornographic Email messages?

15 MR. ADKINS: This is Steve Adkins, Word to the
16 Wise. I've never seen a label on spam, and I've seen an
17 lawful lot of porn spam.

18 MS. LIEB: Rebecca Lieb, Clickz. I second that.

19 MR. LEVINE: This is John Levine. I actually
20 have seen some spam with the sexually explicit label,
21 but I think my recollection is other than the label, it
22 remains completely noncompliant, and I think even some
23 of the stuff that had labels still has indecent pictures
24 actually in the spam, which really defeats the whole
25 point.

1 MR. LEWIS: This is Chris Lewis. We've been
2 filtering on these strings for awhile, and we see a fair
3 number of them. A lot of them are misspelled, and we
4 actually got filters rules in for a number of
5 misspellings and so on. It's been useful. It makes
6 certain pornography spam easier to block, but there's
7 lots of other stuff that comes in without any labelling
8 whatsoever.

9 MR. DAVIS: Chris, let me just clarify.
10 Sometimes the word sexually or sometimes the word
11 explicit is misspelled.

12 MR. LEWIS: The casing is wrong. The hyphens
13 are missing. Most of the time we see things like
14 sexually, colon, explicit. Actually the words
15 themselves are spelled right, but the upper case versus
16 lower case, hyphens versus colons and so on are fouled
17 up.

18 They're better at it than they used to be, but
19 we're still getting lots of pornographic spam that has
20 no labels on them at all. In fact, over the last two
21 weeks, we've gotten 1,368 Email tips of sexually
22 explicit rule that we have, but I would imagine that the
23 number of pornographic spam that we've received is well
24 in excess of 10 or 20 times that that have been caught
25 by other mechanisms or have not passed our filters.

1 So I mean, it's marginally useful but not
2 terribly.

3 MR. DAVIS: What private sector tools exist such
4 as those made available by ISPs or Email service
5 providers to shield consumers from obscene or
6 pornographic Email and how effective is software that
7 can disable links and Email done by those not in the
8 subscriber's address book?

9 How about technology that allows only Email from
10 friends?

11 MR. DELLA PENNA: Mike Della Penna from Bigfoot
12 Interactive. I would say that many of the leading ISPs
13 and Email clients have instituted block images by
14 default on their most recent Email clients that are out
15 there in the marketplace as an attempt to protect
16 consumers on this front.

17 MR. LEWIS: Chris Lewis of Nortel. We have seen
18 spammers who use embedded images in their Email spam as
19 being a way of confirming the user exists and actually
20 just turn around and claim that that's a proof of the
21 user wants the material.

22 So the fact that all of the Email readers now
23 available block images by default is an enormous
24 benefit.

25 MR. DAVIS: Is that the same technology that

1 would replace certain images with text or with neutral
2 characters?

3 MR. LEWIS: Not really. For the most part it
4 inhibits catching the links.

5 MR. DAVIS: Okay.

6 MR. LEVINE: This is John Levine. It may look
7 like it does that. Typically the message has some
8 alternate text to display if the image isn't available
9 so it may look like it's replacing it, but in fact it's
10 just an artifact of what happens when you don't get the
11 image.

12 MR. LEWIS: They have to fill in the hole
13 somehow and it's just the mail reader just throw
14 something up. We are going to be experimenting with
15 some technology that allows us to redirect some of these
16 links to web sites of our own so that we can find out
17 who is doing these fetches and where they're going.

18 MR. ADKINS: Steve Adkins, Word to the Wise.
19 There's a converse to that, which is that the images
20 that are used to get legitimate bulk mail and legitimate
21 individual mail, and the ISPs image blocking that was
22 done out from the demanded users is actually editing and
23 breaking the incoming Email, legitimate Email that the
24 users want to see, and that is causing some significant
25 problems for the legitimate bulk Emailers.

1 They're going on a PR campaign to persuade
2 everybody to add them to their address book, but it's an
3 ongoing operational problem for legitimate bulk mailers.
4 The trade-off is probably worth it, but it's not zero
5 cost.

6 MR. DAVIS: How about technology that the ISPs
7 have created to list sites and Email servers that send
8 pornographic materials, is that perhaps helping?

9 MS. LIEB: I'm sorry, can you repeat that
10 question?

11 MR. DAVIS: Sure. To list sites and Email
12 servers that send pornographic materials help in any
13 way?

14 MR. LEWIS: This is Chris Lewis of Nortel. Do
15 you want to limit it specifically to pornographic
16 materials and things the ISPs themselves have done, or
17 are you implicitly including the use of third-party
18 black lists generally, which is spam, not just
19 pornography?

20 MR. DAVIS: Yes, we can talk about the black
21 lists. Perhaps the related question is: Is there any
22 software or any other option that you're aware of of
23 blocking obscene and pornographic Email that could be
24 anything installed by consumers on their own machines or
25 et cetera?

1 MR. LEWIS: This is Chris Lewis again. We have
2 been doing some evaluations and software exploration on
3 a similar topic. I think it's probably fair to say that
4 many of the anti-spam vendors have been experimenting
5 with policy blocks mechanisms. For example, there are
6 some vendors who are distributing software that would
7 look for skin tones in images.

8 However, as one very major vendor pointed out
9 when he came to visit us, the paint color on the wall
10 would have triggered their detector, and so if we had
11 taken a picture of our president in that room, it would
12 have been caught by their filters, so I think that the
13 technology really isn't there to block it per se. In
14 fact, I think most of the vendors who did try these
15 techniques earlier have since abandoned them.

16 There will probably be yet another waive of
17 attempts at it, but I really don't think that it's a
18 very effective or useful thing at this time.

19 MR. LEVINE: This is John Levine. I've been
20 looking at some of this stuff too, and it turns out it
21 is technically a very difficult problem because the
22 difference between an indecent picture and a decent
23 picture, the difference between a young woman wearing a
24 bathing suit and a young woman not quite wearing a
25 bathing suit is hard enough for people to identify

1 reliably, and I think it's way beyond anything that
2 machinery is going to be able to do.

3 MR. LEWIS: Especially given the wide variation
4 of human intones under various lighting conditions.

5 MR. LEVINE: Yes.

6 MR. LEWIS: Because the wall of the room that
7 I'm referring to is very distinctly orange, not pink.

8 MR. DAVIS: Isn't one of the Sesame Street
9 characters orange?

10 MR. LEWIS: There's a blue one.

11 MR. DAVIS: Okay. Well, our fourth topic for
12 the last 30 to 40 minutes of this teleconference is the
13 effectiveness of various provisions of the CAN-SPAM Act,
14 and there are several provisions, so we would like to
15 just walk through them one by one and discuss whether
16 these provisions achieve their purpose, how effective
17 they have been and whether there are any concerns about
18 the enforcement of any of them.

19 So if you have your copy of the CAN-SPAM Act,
20 you will see that one of the most significant provisions
21 right at the beginning of the Act are the provisions
22 that provide for criminal law enforcement and for
23 criminal penalties, and we would like to invite you to
24 comment on those provisions.

25 MR. DELLA PENNA: Mike Della Penna from Bigfoot

1 Interactive. I think the FTC needs a lot more money. I
2 think some of the efforts to date have been good from a
3 visibility perspective with many of the ISPs bringing
4 suits against spammers, but funding for enforcement is
5 critical, and currently the dollars allocated I think
6 are way too little to accomplish what we need to
7 accomplish on this front.

8 MR. DAVIS: Thank you for that. I would note
9 that the FTC does not have criminal enforcement
10 authority, but I'm sure that your comment is directed at
11 most of the rest of the provisions that the FTC is able
12 to enforce.

13 So with a particular focus on the criminal
14 provisions and the criminal penalty, if anyone has any
15 thoughts on that, we would be grateful for them.

16 MR. LEWIS: This is Chris Lewis of Nortel. As I
17 understand it, there has been one or two prosecutions
18 based on the criminal portions of the code.

19 MR. DAVIS: I believe, yes. I believe it's a
20 number that is not greater than five or six, so, yes.

21 MR. LEWIS: And I'm involved in an effort
22 underway to actually, with law enforcement, to do this.
23 There has been a number of disappointments. Some of the
24 very worst ones of all who we would think would be the
25 easiest to deal with in terms of the criminal portion

1 have not been successfully dealt with.

2 We have been disappointed in that the one or two
3 prosecutions that have even succeeded have been somewhat
4 emasculated by somebody settling early. We have been
5 disappointed by the fact that given the things that are
6 going on in this world today, the various law
7 enforcement agencies don't have the resource to push
8 them as hard as we would like them.

9 It's difficult to see where things could be done
10 differently in terms of the existing law because of the
11 resource constraints that everyone is under, and we
12 need, in many cases, I think laws that allows
13 individuals to act on their own.

14 MR. DAVIS: In other words, private right of
15 action.

16 MR. LEWIS: That's right. In the Canadian
17 federal Anti-Spam Task Force it was acknowledged, it was
18 believed that Canada has sufficient law to deal with all
19 of the things we wanted to in terms of privacy,
20 competition and law enforcement and laws against
21 breaking into machines.

22 So the problem is is that the RCMP is busy
23 dealing with terrorism, gangs, drugs. The Privacy
24 Commission does not have criminal powers. The
25 competitions branch, the best they can do is, Tap

1 someone on the wrist and say Don't do that again.

2 MR. LEVINE: The competition branch of the
3 privacy reverts out.

4 MR. LEWIS: So we have all the things that we
5 need except people who have the resources to actually do
6 it. So the remark that I made in the group was that,
7 yes, it's very nice we have all these laws;
8 unfortunately they're not doing us any good because
9 they're not being enforced, and it would be a really
10 good idea if you gave us the tools to deal with it and
11 got out of our way.

12 MR. ADKINS: Steve Adkins, Word to the Wise.
13 That all sounds great, except I've actually been
14 involved in a couple of cases where fairly rabid anti
15 spammers have taken private legal action against
16 mailers, and it turns out that it was frivolous action.
17 It was being taken purely for harassment.

18 It cost a lot of money, both for the lawyers
19 involved, who were backing it as part of a class action
20 attempt, and for the mailer which didn't appear to be
21 doing anything wrong but still had to defend itself
22 against that frivolous action. There is a downside.

23 MR. LEWIS: Yes, there is a downside. We had
24 long discussions about that specific issue. And we're
25 very cognizant of every single jurisdiction in the world

1 and what laws they have enforced or put in place, and we
2 know the abuses that I think occurred in Utah and some
3 other places, and the lawyers who were in the group who
4 were trying to come up with suggestions and so on came
5 to the conclusion that having seen the way everyone else
6 had implemented these things, having seen the results of
7 them, they were competent they could come up with a set
8 of laws that could not be abused in the way that we had
9 seen them be.

10 So the recommendation has gone forward to the
11 Canadian government is that a private right of action be
12 instituted and there is a considerable amount of
13 material on how it can be framed in such a way to
14 prevent abuse.

15 MR. COHEN: This is Jordan Cohen from Bigfoot
16 Interactive. I realize the conversations has moved a
17 bit away from the original question about the criminal
18 provisions purely, but we certainly would be concerned
19 as a legitimate sender for Fortune 500 companies, if
20 there was such a private right of action in the law.

21 Just going back to the enforcement, again I
22 reiterate what Michael said earlier about the need for
23 stepped up enforcement, but to date we do think that the
24 provisions of the Act have been enforceable as
25 demonstrated by the estimated 200 to 300 actions, both

1 civil and criminal, that have been taken to date.

2 I did read the comments of the Internet Commerce
3 Coalition, the ICC, in response to the latest NPRM up on
4 the FTC's web site, and in fact, it's an industry
5 coalition of ISPs who are also empowered to take
6 enforcement action and have taken they say about 150
7 actions, so there certainly is the ability to enforce
8 this. It's just a matter of keeping that persistent.

9 Again all of this will be fruitless without
10 publicity of those enforcement actions, such as for
11 example when AOL, when there was somebody who had stolen
12 90 million Email addresses from AOL, having that in the
13 national news for a full week and the fact they actually
14 nabbed this person, showing his picture on T.V., things
15 like that will continue to be helpful, but we just need
16 to keep it persistent.

17 What the FTC did last week taking actions
18 against the pornographic spammers, and importantly
19 affiliates and the actual advertisers behind the
20 affiliates, the tons of publicity that that got. We
21 just need to continue efforts like that, and Bigfoot
22 Interactive believes that enforcement, both civil and
23 criminal, with publicity will be fruitful.

24 MR. LEVINE: John Levine. I was part of the
25 case that put spammer Jeremy Jaynes in jail in Virginia,

1 and although that was under the Virginia state law, its
2 criminal provisions are fairly similar to the ones in
3 CAN-SPAM, and what I took away from that was that it was
4 great that we put this guy in jail, and he certainly
5 deserved it but the cost of preparing and prosecuting
6 the case was enormous, and the Commonwealth couldn't
7 have done it if AOL hadn't put an enormous amount of
8 their own resources into collecting the evidence and
9 basically educating the prosecutors and the court about
10 what was going on.

11 So that although criminal provisions may be
12 useful for a handful of the most enormous spammers, it's
13 way to expensive to use as a general anti-spam device,
14 which brings us back to Chris's point, that we need to
15 be able to do civil suits at modest costs, which brings
16 us right back to private right of action.

17 MR. DAVIS: Well, why don't we move off the
18 criminal provisions and penalties and then delve into
19 the numerous civil provisions, starting off first with
20 the prohibition on false header information, which
21 applies to commercial and transaction type messages.
22 Any thoughts on that false header provision?

23 MR. LEVINE: John Levine. That's basically what
24 we nailed the guy in Virginia on, and there's no
25 conceivable reason for anybody to be sending mail

1 legitimately with false headers, but really all that
2 does is to simplify the education process a little bit
3 because any mail with false headers invariably is
4 fraudulent in other ways, and so the sender is
5 invariably breaking more general fraud or computer crime
6 laws so it's nice, but it's not a big deal.

7 MR. ADKINS: Steve Adkins. We've actually had
8 or dealt with a number of people that were sending false
9 header information inadvertently. There's a lot of
10 people sending legitimate bulk mail out there who aren't
11 very competent at it, so there's not actually
12 100 percent correlation between fake headers and it
13 being legitimate Email, but the vast majority is
14 certainly not legitimate mail, and it's a wonderful
15 very, very simple hook to hang legal action on.

16 MR. LEWIS: This is Chris Lewis. The difficulty
17 being defining what some of that stuff is. We discussed
18 this long and hard in the Asset Group about false
19 headers and so on, and basically what we came to the
20 conclusion on was that some of it is useful, from a
21 competition small advertising perspective.

22 Some what we did suggest was that it would be
23 more useful if we had stronger provisions when you are
24 spoofing, being someone else, so if you're using random
25 garbage front lines or misleading subject lines and so

1 on, that's one thing, but if you're impersonating
2 somebody who exists, there should be stronger and it
3 should be easier to have stronger measures in place.

4 MR. COHEN: This is Jordan Cohen from BigFoot
5 Interactive. I think that the falsified header
6 provision is one of the most important in the Act, at
7 least leading up to enacting it in late 2003. America
8 Online, at least in their perspective, testified that up
9 to 90 percent of what they considered spam contained
10 falsified header and routing information.

11 Just a few months later the Senate Commerce
12 Committee held a hearing about the effectiveness of the
13 Act -- about six months later -- and I believe her name
14 was Jana Monroe from the FBI, testified that before the
15 CAN-SPAM Act, the FBI was reluctant to get involved in
16 spam whatsoever, but because of provisions like
17 falsified header, no use of proxies and relays, forgery,
18 that sort of thing, the Act of spamming on its face
19 became illegal, so we think that again that provision
20 directly targets up to and perhaps even more than
21 90 percent of the problem.

22 MR. DAVIS: Why don't we move on to the
23 provision against deceptive subject lines. Any comments
24 on that with regard to the effectiveness or enforcement
25 of the CAN-SPAM Act?

1 MR. ADKINS: Steve Adkins. I still see that as
2 a very hard to define thing, particularly given the
3 history of bulk marketing. A lot of otherwise perfectly
4 legitimate Emails being sent out that isn't spam, but
5 it's covered under the CAN-SPAM guidelines, conformed in
6 every other respect, but the subject lines are still
7 arguably misleading, so I think it's the bit that's most
8 ignored. It's nice to have, but it's not something
9 people pay as much attention to as the other provisions.

10 MR. DAVIS: The next provision is a requirement
11 that Email messages, including functioning return
12 address or an other opt-out mechanism, and it must work
13 for 30 days, and there's a safe harbor for temporary
14 unavailability. Any thoughts on that provision?

15 MR. CASTELLI: This is Eric Castelli with
16 LashBack. Yes, I don't know where to start. First of
17 all, hopefully your most recent NPRM will address this,
18 but there's way too much ambiguity about what
19 constitutes an opt-out mechanism. We've got a whole
20 myriad of different opt-out mechanisms which creates
21 confusion for consumers, and often are used to prevent
22 the user from opting out.

23 Also, as I think I mentioned before, one of the
24 big problems that unsubscribe faces, which I believe is
25 a huge tenet of CAN-SPAM, is there's nothing to protect

1 the consumer from having their request to unsubscribe
2 from being misused. As far as I know, CAN-SPAM does not
3 make it illegal for an individual to take the
4 suppression list of another company and send mail to it.
5 That obviously puts consumers in a very bad situation
6 where the very thing CAN-SPAM tells them to do, which is
7 unsubscribe, actually yields them more spam.

8 Also, as an organization, LashBack has discussed
9 unsubscribe compliance failure with many organizations
10 which we have data on, and the common consensus is "We
11 don't care." They feel that the FTC will not act on
12 that information, and I largely believe that the failure
13 to act by the FTC on an unsubscribe basis has been
14 related to lack of funding, but as it stands now, the
15 tenet of CAN-SPAM, which is unsubscribe, is a joke.

16 There are legitimate businesses, and most of the
17 legitimate advertisers are playing by the rules when it
18 comes to unsubscribe -- but not are all out spammers not
19 being compliant. But some of the large affiliate
20 networks are just breaking the rules, and they are not
21 suffering the consequences.

22 MS. HARRINGTON-MCBRIDE: Eric, this is Katie.
23 Would you give us some examples of ambiguous opt-out
24 mechanism, some of the variety that you're seeing.

25 MR. CASTELLI: Well, there's two scenarios I

1 think I discussed before. One is you submit your Email
2 address to an opt-out link, and we test this by seeding
3 opt-out links throughout the Email community, and when
4 submit your Email list, the suppression list is taken
5 and either intentionally or unintentionally people start
6 mailing the suppression list.

7 Not only does this happen with the slime balls
8 that don't even put a physical address in the Email, but
9 you see it very commonly with the big ad networks, and
10 if you'll permit me, I'll say Azoogole is a large ad
11 network that this happens to. We contact the ad
12 network, and they don't care. So the affiliate networks
13 aren't taking accountability for what's happening. The
14 advertisers aren't and the senders aren't, so it's just
15 a big joke to them.

16 Then of course the other side of the equation is
17 whether or not they're honoring requests within ten
18 business days, and that's not happening either.
19 LashBack is an organization that feels that the FTC has
20 the tools and the information, but thus far we have seen
21 no action.

22 So CAN-SPAM is not about unsubscribe. It's
23 about porn and falsified headers, so spammers continue
24 to have the right to spam, and there's no enforcement
25 around that basic premise.

For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555

1 MS. HARRINGTON-MCBRIDE: One more follow-up
2 question. Katie again.

3 MR. CASTELLI: Sure.

4 MS. HARRINGTON-MCBRIDE: You mentioned that
5 there's a view of opt-out is occurring often in the
6 affiliate context. There is a provision of the Act, and
7 I wonder if you have any specific thoughts about it
8 efficacy. It's the provision within opt-out which
9 prohibits the sending after ten days of Email to an
10 address which has opted out, and it makes it
11 specifically prohibitive for the sender or any other
12 person who knows that the recipient has made an opt-out
13 request to sell, lease, exchange or otherwise transfer
14 or release an Email address of the recipient, and it
15 sounds to me like what you're saying is that that has
16 not been an effective deterrent, but I want to clarify
17 that.

18 MR. CASTELLI: That's correct. I have been
19 working with your organization and chatted with
20 different people there. My understanding is that based
21 on the current law, when a third-party steals a
22 suppression list or takes it and sends Email to it, they
23 are not breaking the law. I could be misinformed and
24 mis educated, but that's my current understanding, and
25 if it is the law that they can't do it, they're

1 certainly not abiding by it.

2 MR. ADKINS: Steve Adkins. When you're dealing
3 with affiliate networks, when you're dealing with
4 out-sourced mailing, there's to some degree a
5 requirement of CAN-SPAM to share those suppression
6 lists. If you have multiple mailing from the same list
7 to different recipients, then if someone had opted out
8 of that mailing, then that suppression list needs to be
9 distributed amongst everybody mailing to that, and I
10 think that's where a lot of the suppression lists are
11 distributed.

12 From that point on they're also traded and sold
13 between mailers, both these suppression lists and
14 presumably sometimes mis marked as lists of addresses.

15 MS. HARRINGTON-MCBRIDE: Steve, you have raised
16 a good point. This is Katie again. I stopped short
17 with reading that provision of the report. It does say
18 for any purpose other than compliance with the Act, so
19 in sharing the information, to the extent that you're
20 doing it, to ensure the correction occurs is
21 permissible, but to do it for any other reason
22 obviously, especially to do it in order to send more
23 Email, would be prohibited.

24 MR. ADKINS: Yes, Steve Adkins, but that
25 requirement ensures that those suppression lists will be

1 distributed very widely, and they will be shared with a
2 lot of people, in particular with affiliates or major
3 out-source program, which pretty much guarantees that
4 they will get in the hands of someone who will misuse
5 them sooner or later.

6 MR. CASTELLI: Eric Castelli again with
7 LashBack. I agree. So the problem is they're trying to
8 comply with the law, that's good, but when the law is
9 broken by this third-party that takes the suppression
10 list, my understanding is their act is not a violation
11 of CAN-SPAM.

12 MS. LIEB: This is Rebecca Lieb from the Clickz
13 Network. Just to amplify that, I think everybody would
14 benefit a lot more rules surrounding the use and the
15 abuse of suppression lists, not only in terms of the
16 abuses that we've just been discussing which certainly
17 happen, and I know Jordan and Michael are probably going
18 to chime in here, but also in light of the shelf life of
19 a suppression list. Many marketers that I've been
20 speaking with would like to see some sort of sunset
21 provision applied to opt-out, given the amount of Email
22 churn in the industry.

23 So I think many, many questions regarding once
24 somebody has landed on a suppression list, how long do
25 they stay there, how confined is that information and

1 what's the shelf life of that list have yet to be
2 defined.

3 MR. COHEN: You're right. Jordan Cohen from
4 Bigfoot Interactive, but before getting into that, I
5 would like to observe that at least in the legitimate
6 marketing community, I think that we have a very -- that
7 we have decisive clarity about what should be done with
8 opt-out and suppression, and I think that I've read
9 articles from Mr. Castelli before, and as he points out,
10 this is before the Act and it will continue to be the
11 case in the years to come, the bad guys aren't going to
12 comply with any of the provisions really, but the good
13 guys are complying.

14 It's certainly with the opt-out, and we're
15 supportive of the current ten-day framework, but in
16 terms of managing, processing the opt-outs between
17 affiliates when it's necessary, all that's being done by
18 legitimate businesses that care about the law and care
19 about compliance, so we do think that that's working,
20 and the fact that so many spammers are doing it
21 (violating the opt-out provision) just heightens the
22 need for continued enforcement of the existing statute.

23 With that said, following what Rebecca said, we
24 submitted comments along with many other associations
25 and legitimate marketers and Email service providers

1 requesting that there would be some sort of sunset
2 provision for the opt-out.

3 Our research also found that Email addresses
4 churn on average about 20 percent per year, which means
5 that within five years most suppression lists are going
6 to be composed of non functional address, but under the
7 current law, that still doesn't mean that we won't be
8 scrubbing against them, so what we're faced with right
9 now, it isn't a huge problem today, but we are concerned
10 that in the future, in the very short-term future that
11 we're going to be using substantial database resources.
12 Scrubbing against lists takes a pretty long amount of
13 time, delaying the process of marketing legitimately, so
14 that's an area where we think that the Act could be
15 improved.

16 MR. DELLA PENNA: In addition to Jordan's
17 comments, Mike Della Penna, Bigfoot Interactive. The
18 average consumer reported to us that they have two and a
19 half Email addresses, which adds to the complexity, cost
20 and processing requirements as it relates to the
21 suppression issues.

22 So this is something that we're looking at very
23 closely and tracking accordingly, but again there have
24 been no issues right now as far as compliance with the
25 current provision. It's just that we need to be

1 conscious about the sunset provisions as it relates to
2 an emerging medium that is changing and evolving each
3 and every day.

4 MR. LEVINE: This is John Levine. I strongly
5 oppose a sunset provision. I've had the same address
6 for 13 years which is a bit extreme, but I know I'm far
7 from the only person who keeps an Email address for a
8 long time, and I know a lot of people who deliberately
9 get an address at a place like POBox.com or use an
10 address at a professional association or a college
11 alumni association, specifically so they can have a
12 consistent long-term address that their friends and
13 correspondents can use, and I think the assumption that,
14 Oh, the addresses all go away in five years is simply
15 wrong, and it would be bad policy to enact that into
16 law.

17 MR. DELLA PENNA: Mike Della Penna from Bigfoot
18 Interactive. I would just add that there is a dramatic
19 move to broadband, and I think you are the exception
20 rather than the rule. There continues to be price
21 competition as it relates to Email services and
22 providers. The move to broadband is the fastest adopted
23 technology that the industry has ever seen, and that
24 continues to impact Email churn quite dramatically.

25 MR. ADKINS: Steve Adkins. I would agree that

1 most broadband is significant, and that's one of the
2 reasons more and more people are actually going to third
3 party services, including companies like Outblaze,
4 Hotmail, Yahoo Mail, specifically so they can have a
5 long-term consistent Email address, even though they are
6 moving from provider to provider.

7 I think from talking to people who have changed
8 Email addresses, one of the major drives I'm seeing for
9 people actually changing Emails is when an Email address
10 becomes unusable because of the amount of spam, that's
11 when they change it. It's not necessarily driven by
12 them changing ISPs in a lot of cases.

13 MR. DELLA PENNA: Mike Della Penna from Bigfoot
14 Interactive again. Our research is contrary to that.
15 Last year in 2003 the number one reason for switching
16 ISPs or Email service providers was spam and price.
17 This year our research indicated that it was the move to
18 broadband and price. Spam significantly decreased as a
19 reason for switching ISPs, so from what we're hearing
20 from consumers and seeing from our research, that is not
21 the case.

22 MR. LEWIS: This is Chris Lewis. Switching to
23 broadband --

24 MR. DAVIS: I'm sorry?

25 MR. LEWIS: Switching to broadband because of

1 availability, once you've done it, you're not likely to
2 move much again, so I mean, this is an evolutionary step
3 because of the availability of a new access service, but
4 once those are saturated we're going to get back to the
5 same situation where people's Email addresses will start
6 becoming more polluted with more spam.

7 MR. DELLA PENNA: Except price will continue to
8 be an issue.

9 MR. COHEN: Jordan Cohen from Bigfoot
10 Interactive again. The record certainly reflects
11 looking over the NPRM comments that several commentators
12 indicated that beyond just -- there's our research and
13 there's other research that indicates significant Email
14 address churn, but even just marketers own experiences,
15 we saw banks saying that they just detect on their own
16 that like 30 percent of their customers change email
17 addresses every year.

18 Again the key is that legitimate marketers will
19 always abide by whatever the rules are, and whether it's
20 five years or some sort of other established time frame,
21 if by chance somebody gets added to a legitimate
22 marketer's list and they ask to opt-out, I'm sure that
23 marketers will do that today as they will say five years
24 from now.

25 Again we just request that the Commission

1 carefully considers balancing both the interests of
2 legitimate business and consumers here. Again
3 legitimate businesses will always honor the opt-out. At
4 the same time, we really do believe that it's onerous
5 and a problem in the making if marketers end up having
6 lists of literally millions, hundreds of millions of
7 addresses that are non functional they have to scrub
8 against.

9 That's just a fact on the ground in terms of
10 legitimate marketing today.

11 MR. DAVIS: Well, there's one additional
12 prohibition the Act requires, and I'll just ask if there
13 are any other comments on the ten-day period after which
14 transmission of commercial Email after an opt-out is
15 prohibited?

16 MR. CASTELLI: This is Eric Castelli with
17 LashBack. I wanted to give some feedback here, and I
18 did this on the response for the NPRM recently, but one
19 of the concerns about the ten-day period was that it was
20 too long and that during the opt-out period, marketers,
21 senders, and advertisers had the ability to mail bomb a
22 consumer during that period.

23 I stipulated this in my response, but also
24 wanted to reaffirm it by saying that I have never seen,
25 and as a company we've never seen, individuals being

1 bombarded during the opt-out period. And that said,
2 legitimate marketers are the ones that are complying,
3 and they are the ones that have a difficult time
4 complying, and the ten-day period is sufficient I think
5 for consumers, and it's a challenge also for advertisers
6 and senders. So I don't see a need to change it to
7 three business days.

8 MR. ADKINS: Steve Adkins. Ten days is very,
9 very tight in terms of handling the amount of data
10 involved with mailers. It's not a trivial operation to
11 do. Mail shops are prepped days, sometimes a week or
12 two in advance. 30 days, no problem at all. Ten days
13 is doable, but not trivial that's required changes in
14 operational behavior. Going much shorter than ten days
15 would actually put an undue burden on legitimate
16 senders.

17 MR. DAVIS: Okay. Well, there is a provision in
18 the Act that has three parts, and the first part is a
19 requirement that commercial Email include an identifier,
20 any thoughts on that provision?

21 MS. LIEB: Rebecca Lieb from Clickz. I think
22 the term advertisement is simply too ambiguous, and
23 ill-defined. Is it a marketing message, is it a
24 transaction message, what if it's a statement from your
25 bank account or your brokerage house that perhaps has an

1 ad for extra products and services within it? I think
2 advertisement or a label in that direction is something
3 that could be more easily flittered than used
4 effectively.

5 MR. DAVIS: How about the requirement that there
6 be clear and conspicuous notice of the opportunity to
7 opt-out, so to speak, to decline to receive further
8 Email?

9 MR. ADKINS: Steve Adkins. I think that's a
10 good thing, and it just encourages the good players to
11 clarify their behavior there. It's something we're
12 pretty much all doing anyway. I don't think it has much
13 effect on the bad players.

14 MR. CASTELLI: Eric Castelli with LashBack.
15 Even more clarification needs to be brought to that I
16 think. As Steve pointed out, the good guys are doing
17 it. They're labeling it very clearly, and they're
18 making their unsubscribe a fairly easy process, but
19 currently there's no standards, there's a complete lack
20 of clarity on what constitutes a clearly defined
21 mechanism. So I think more clarity needs to be brought
22 to the requirement and almost specific requirements
23 about how it's labeled or the processes involved to
24 unsubscribe which I applaud the recent proposals in the
25 NPRM about reducing the amount of information required.

1 MR. DAVIS: There's one more disclosure
2 requirement, and that is for the commercial Email to
3 include the valid physical postal address of the sender.
4 What do you think about that? Is that effective or
5 enforce able?

6 MR. LEVINE: This is John Levine. It's one of
7 the ones that you have the hardest time getting right.
8 I don't see it as particularly effective either way.

9 MR. ADKINS: Yes. The main use I make of that
10 is whether they get it right or not is a very get metric
11 of how closely they're paying attention to the CAN-SPAM
12 requirement, but that's the primary value of it.

13 MR. DAVIS: Let me ask about the penalties that
14 the Act provides. Do you think that those penalties are
15 a deterrent? Are they effective?

16 MR. ADKINS: Steve Adkins. Amongst the bad
17 players, clearly not. I think amongst the good players,
18 the actual ones that want to get it right, I think
19 honestly the penalties are less of a disincentive in
20 themselves as, Oh, my, we don't want to seem to be
21 breaking the law, we want to comply with the law, so for
22 the people who are going to comply with it, the
23 penalties aren't the critical bend.

24 For the people that aren't going to comply with
25 it, they don't care anyway. The time the penalties come

1 into play is when somebody is doing something bad, they
2 give you something additional to levy against and get
3 legal action.

4 MR. DAVIS: There are certain sorts of
5 aggravated violations that can occur, and the Act deals
6 with them. I believe harvesting and dictionary attacks
7 are among them. Do you feel that those provisions are
8 effective.

9 MR. ADKINS: Steve Adkins again. All the spam I
10 get comes to harvested addresses. They are harvesting.
11 That's basically what is going on. Nothing is going to
12 prevent the spammers who are perpetual violators of the
13 provisions from violating that as well. The additional
14 aggravated damages is, is it going to prevent them from
15 doing it. Again it just means it's a useful tool when
16 you do actually take legal action against them. I don't
17 think it's much of a disincentive prior to that.

18 MR. DAVIS: It also addresses automated creation
19 of multiple Email accounts and the zombies, the relay or
20 retransmission through unauthorized access.

21 MR. ADKINS: Steve Adkins. As Chris said
22 earlier roughly 80 percent of the spam he's seeing is
23 violating that point, so it's clearly not having that
24 much of an effect on the majority of Spammers.

25 MR. DAVIS: You know the Act also directed the

1 FTC to engage in a rulemaking, and as a result, we had
2 the April 2004 sexually explicit label requirement and
3 the Brown Paper Wrapper requirement. I think that the
4 group has already commented on that and its
5 effectiveness, but if anybody would like to add
6 anything, this would be a great time to do that.

7 Okay. There's also a prohibition in the Act on
8 promotion of a person's trade or business in a
9 commercial Email message, the transmission of which
10 violates the provision against false or misleading
11 header information, et cetera, and this is a provision
12 that the FTC only is able to enforce.

13 Do you have any thoughts about the effectiveness
14 of that particular provision of the Act?

15 MR. LEVINE: I think it's the same answer.
16 Basically it's a piling on of the provision. Anybody
17 who is has violated that has violated a bunch of other
18 things, so I don't think by itself it makes much
19 different.

20 MR. DAVIS: That's John Levine?

21 MR. LEVINE: Yes.

22 MR. DAVIS: Another provision of the Act deals
23 with preemption of state laws, except those that are not
24 specifically Email. Any thoughts about the preemption
25 aspect of the CAN-SPAM Act?

1 MR. COHEN: Jordan Cohen from Bigfoot
2 Interactive. Definitely with the confusion that we've
3 had to face here over the last few weeks with what's
4 going on in Utah and Michigan, that's certainly
5 something that we're concerned about. We think it's
6 very clear, however, but our understanding is that the
7 only way for the preemption to take effect in these
8 states would be for there to be a lawsuit, which nobody
9 obviously wants to get involved with.

10 So we definitely hope that there is some way for
11 the government or the federal government to be a bit
12 more clear to the States because although we've worked
13 with lawyers to clarify and explain these laws to our
14 client base, it certainly is something that will
15 continue to cause confusion and create problems in the
16 legitimate marketplace unless, there's decisive clarity
17 there.

18 We do think that the preemption was a critical
19 component to the CAN-SPAM Act. It's critical to have a
20 national standard, and we think that that's a good one.

21 MR. DAVIS: The final provision required the
22 Federal Communications Commission to promulgate a rule
23 relating to commercial messages received on cell phones
24 and mobile devices, wireless rulemaking so to speak.
25 Any thoughts of the effectiveness of that?

1 MR. ADKINS: Steve Adkins. When I checked on
2 that, it was all a bit ill-defined, and the number of
3 providers who were not wireless providers appeared to
4 have signed to be listed as wireless providers, so there
5 seems to be some confusion in the operation there.

6 MR. DAVIS: Okay. Well, thank you all for
7 joining us on this call today from your various offices
8 and your various times zones.

9 If you have any data sources, any sort or type
10 of study or article or reference to a particular person
11 that you think that we might not be aware of and you
12 would like to make us aware of, please let us know.
13 I'll give you my Email address again in a second, and
14 also if you have any further thoughts on these issues,
15 please let us know.

16 We would request to hear from you within about
17 three weeks, say, August 15, and you can reach me at
18 Email address mdavis@ftc.gov, M D A V I S @ F T C . G O
19 V.

20 Once the transcript of this call is available,
21 we will circulate that to all of you so that you may
22 have an opportunity to review it and correct. Because
23 there are so many participants on our various calls, it
24 would be most helpful for you to make any corrections in
25 a red line format and send us that red line, and we'll

1 also be asking for a fairly quick turnaround. our
2 investigator, Allyson Himelfarb, is the contact person.
3 She is the person who sent you the Email inviting you
4 and confirming your attendance for the calls today.
5 She'll be in touch with each of you as soon as the
6 transcript is ready.

7 So I thank you again for participating in this
8 call. Your input has been very helpful and it will
9 assist us in completing the report to Congress on the
10 effectiveness and enforcement of the CAN-SPAM Act.
11 Thanks so much.

12 (Whereupon, at 12:02 the conference was
13 concluded.)

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

1 CERTIFICATE OF REPORTER

2

3 DOCKET/FILE NUMBER: P044405

4 CASE TITLE: REPORT TO CONGRESS

5 HEARING DATE: JULY 26, 2005

6

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

12

13 DATED: AUGUST 8, 2005

14

15

16

DEBRA L. MAHEUX

17

18

CERTIFICATION OF PROOFREADER

19

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

23

24

DIANE QUADE

25