

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

FEDERAL TRADE COMMISSION

I N D E X

INTRODUCTION	PAGE
BY MS. HARRINGTON-MCBRIDE	4

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

FEDERAL TRADE COMMISSION

IN THE MATTER OF:)
CAN-SPAM REPORT TO CONGRESS.)
) Matter No.:
) PO44405
)
-----)

THURSDAY, JULY 21, 2005
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

The above-entitled matter came on for
conference, pursuant to agreement, at 10:06 a.m.

1 APPEARANCES:

2

3 ON BEHALF OF THE FEDERAL TRADE COMMISSION:

4 CATHERINE HARRINGTON-MCBRIDE, ESQ.

5 MICHAEL DAVIS, ESQ.

6 ALLYSON HIMELFARB, INVESTIGATOR

7 600 Pennsylvania Avenue

8 Washington, D.C. 20058

9

10 ALSO PRESENT VIA TELEPHONE:

11 BEN EDELMAN, Harvard

12 JOE STSAUVER, University of Oregon

13 STEVE BELLOVIN, Columbia

14

15

16

17

18

19

20

21

22

23

24

25

P R O C E E D I N G S

- - - - -

1
2
3 MS. HARRINGTON-MCBRIDE: Good morning, everyone.
4 Thanks so much for joining us on this call this morning.
5 I apologize, we're a couple minutes late dialing in. We
6 had a little technical difficulty, but I think we're all
7 squared away now. We have a court reporter with us.
8 Debbie, are you all set to go?

9 MS. MAHEUX: Yes, I am, Katie. Thank you.

10 MS. HARRINGTON-MCBRIDE: Great. When I say with
11 us, I sort of mean as in with us along the phone wires
12 because Debbie is actually calling into the call as
13 well.

14 I will go ahead, and just for purposes of
15 establishing the record, take roll call if that's okay.
16 You guys being academicians, I know you're familiar with
17 seating charts and figuring out who all is in the class,
18 and this is a small class.

19 Ben Edelman, are you with us?

20 MR. EDELMAN: I am.

21 MS. HARRINGTON-MCBRIDE: Terrific, thank you.
22 Joe StSauver?

23 MR. STSAUVER: Here.

24 MS. HARRINGTON-MCBRIDE: Thanks, Joe. And Steve
25 Bellovin?

1 MR. BELLOVIN: I'm here.

2 MS. HARRINGTON-MCBRIDE: Great, thank you. My
3 name is Katie Harrington-McBride. I'm an attorney with
4 the Division of Marketing Practices at the Federal Trade
5 Commission. I know I've met some of you in the past by
6 phone at the very least, and I am working right now on
7 the report to Congress on the effectiveness and
8 enforcement of CAN-SPAM, along with two colleagues who
9 join me: Michael Davis, an attorney in our division,
10 and Allyson Himelfarb, an investigator.

11 We're grateful that you've joined us to talk
12 about these issues because it will no doubt further our
13 ability to produce a very effective and informative
14 report to Congress.

15 As you all know, in December of 2003, Congress
16 enacted and the President signed the CAN-SPAM Act, which
17 among other things directs the FTC to report on the
18 effectiveness and enforcement of the CAN-SPAM Act no
19 later than 24 months after the passage of the Act, so
20 the report is due to Congress by the middle of December
21 of this year.

22 Since the passage of the Act, the FTC has been
23 in the process of gathering data, establishing baseline
24 data and obviously trying to gather any data we can that
25 would impact or demonstrate the effect that the Act has

1 had on the world of Email practices and certainly on
2 spam.

3 This interview with academics will be
4 transcribed for the record and will be a part of the
5 record for the record. This interview today is just one
6 of the ways that the FTC is seeking information that
7 will be relevant for the report on the effectiveness and
8 enforcement of the Act.

9 Because today's call is being transcribed for
10 the record by a court reporter, who is listening to the
11 call, it's very very important that when you wish to
12 speak, you begin by stating your name and affiliation.
13 I think in fact because we all have distinct first
14 names, it's probably okay to just identify yourself by
15 first name for the purposes of today's call. If you
16 don't remember, we'll try to remind you so that we can
17 keep the record clean, and we know who said what.

18 I just want to be absolutely clear that your
19 views expressed today will be transcribed for the record
20 and may be appended to the report to Congress or
21 otherwise made public. I just want to be sure everyone
22 is clear on that.

23 Are there any questions before we begin?

24 Okay. Let me give you a sense of the outline
25 for the call. We've scheduled two hours, and I can tell

1 you that because of past calls we've done, we've been
2 coming in anywhere between an hour and 20 minutes and
3 actually two hours, so we certainly won't go over two,
4 but we would like to cover four main topics.

5 The first is marketplace developments or
6 technological changes since the passage of the Act in
7 December of 2003 that may affect the practicality or
8 effectiveness of the Act. This language is taken
9 directly from the CAN-SPAM Act, the provision that
10 requires that the FTC submit a report at two years out,
11 and it's one of the specific areas that Congress desires
12 analysis on in our report, so we'll talk about that in
13 some depth.

14 We'll also talk about a second issue that
15 Congress is interested in, and that is the extent to
16 which the international transmission of Email may affect
17 the effectiveness of the Act and any suggestions for
18 change.

19 Our third issue today will be ways in which
20 consumers, particularly children, can be protected from
21 obscene and pornographic material, and finally we'll
22 talk about the effectiveness of various provisions of
23 the Act, discussing each provision individually. We'll
24 also talk about the enforcement of those provisions and
25 any impediments.

1 So for each of these areas, I'll ask a series of
2 questions, and if you have any information that you
3 believe to be responsive or if it triggers you to think
4 of an additional question, just signal your interest
5 verbally. Let us know that you're interested in
6 talking, and we'll go ahead and call on you, and you can
7 state your answer for the record.

8 It has worked out fairly well, despite the fact
9 that none of us can see one another in past calls, so if
10 we start to end up in a pile up, we'll try to figure out
11 a better way to go, but for now if you have something to
12 say, just feel free to jump in, state your first name
13 and answer.

14 So with that I guess we can start with our first
15 issue, that is, whether there are any marketplace
16 developments or technological changes since the passage
17 of the Act that may affect the practicality or the
18 effectiveness of the Act, and we've broken it down into
19 a couple of specific questions, but if you have any
20 general thoughts, we'll be glad to hear those as well.

21 MR. BELLOVIN: This is Steve.

22 MS. HARRINGTON-MCBRIDE: Hi, Steve.

23 MR. BELLOVIN: To me the biggest change over the
24 last couple of years has been the move towards other
25 forms of illegality in spreading spam, violations of

1 computer fraud and abuse, hacking people's PCs, turning
2 into spam engines, as well as more sophisticated
3 technical mechanisms to try to launch spam and avoid
4 detection.

5 I think it's not possible to think about
6 economic solutions to the spam anymore, for example,
7 because it would be penalizing innocent parties or at
8 least partly as we think about them.

9 MS. HARRINGTON-MCBRIDE: Is that because of the
10 presence of zombie drones?

11 MR. BELLOVIN: Exactly.

12 MR. EDELMAN: This is Ben Edelman. As to
13 zombies, I certainly share Steve's sense that this is a
14 large and growing problem. It's worth noting the ways
15 that this overlaps with other matters within the
16 Commission's subject matter of interest and purview. In
17 particular, many of these drones are also being
18 implemented and designed to put in place with a goal of
19 installing Adware or Spyware on users' computers, so
20 we've got a combined profit motive from definite illegal
21 spam transition plus probably illegal installation of
22 unwanted advertising software.

23 The Commission's ability to do something about
24 one might tend to undermine the economic incentives that
25 have given rise to the other and vice versa.

1 MS. HARRINGTON-MCBRIDE: Okay. Thanks, Ben.

2 MR. STSAUVER: This is Joe. I would suggest the
3 rise of affiliate programs has contributed to the
4 problem more so than some of the other things that may
5 be happening on the technological level.

6 MS. HARRINGTON-MCBRIDE: Okay. One of the
7 questions I guess that we're going to try to get at is:
8 In what ways may the Act be deficient and could it be
9 improved, or are the developments -- I mean, to some
10 extent I think it's clear from both the Congressional
11 Record when the Act was passed and from public
12 statements by members of the Commission at the FTC that
13 the legislation is not perceived by most as a silver
14 bullet solution to the problem of spam.

15 Instead, I think many think that there have to
16 be collaborative efforts between technologists and law
17 enforcers and likely those in the industry to
18 effectively free up folks' mailboxes in a way that would
19 be advantageous for recipients, and I guess to some
20 extent today, I would ask you to think about whether in
21 answering these questions, if you have any thoughts
22 about specific ways in which the Act, as it is written,
23 may be deficient given changes that have happened in the
24 last 18 months, and any practical suggestions that you
25 might have for improvement.

1 So that's just sort of an umbrella comment, but
2 you guys are off to the races on this. It's clear that
3 you've all thought about this a lot, so this is going to
4 be a good call.

5 One of the specific questions Congress has asked
6 us is whether there are new or increasingly used --
7 well, they asked specifically about ways in which
8 recipients receive Email, so we interpret that to mean
9 are there new or increasingly used methods for receiving
10 Email that impact in any way the effectiveness of the
11 Act, and you might think here about the use of cell
12 phones and other mobile devices to view Emails, and
13 whether the size of the screen or other technological
14 impediments make some of the protections of the Act less
15 effective.

16 Any thoughts about that?

17 MR. STSAUVER: This is Joe. I think in many
18 cases the wireless providers are less likely to provide
19 full headers on messages that are transmitted to
20 wireless users, so as a result, it's harder for folks to
21 truly decide what is actually being sent to them to
22 actually see where it is coming from, and of course the
23 wireless devices also tend to be less configurable.

24 You have fewer options. You couldn't run
25 something like Spam Assassin on a wireless device as an

1 individual user.

2 MS. HARRINGTON-MCBRIDE: Okay.

3 MR. BELLOVIN: Yes, there's a growing issue
4 of -- I don't know if it's technically spam within the
5 meaning of the Act, but spam over other media, IM
6 systems, SMS messages and the like. SMS messages are
7 particularly worrisome because the number of people who
8 actually pay per message received. Do you want me to go
9 into the fourth coming threat of SPIT, spam over
10 Internet telephony?

11 MS. HARRINGTON-MCBRIDE: They all have
12 delightful names, don't they? That's Steve, right?

13 MR. BELLOVIN: So that will be a concern going
14 forward, but the mobile devices, I suspect that some of
15 them are actually seeing weird stuff instead of the spam
16 itself because you're not going to transmit a large HTML
17 attachment to many of these devices. A lot of the spam
18 I get has strange and wonderful text bayesian filters
19 and plain text and the actual content in HTML or an
20 attached image in an alternate content.

21 So it's going to be confusing and annoying but
22 in a different way. It won't be, for example,
23 pornographic in many cases.

24 MS. HARRINGTON-MCBRIDE: Okay. Joe, something
25 you said triggers another question in my mind, and that

1 is you mentioned you can't run programs like Spam
2 Assassin on a mobile device. Are there any products
3 that any of you are aware of that are specifically
4 targeted to protect mobile devices from unwanted
5 messages, or is that all done through the carriers?

6 MR. STSAUVER: That's really a carrier level
7 function, and I think it's also worth noting, of course,
8 that wireless devices do enjoy some special protection.

9 MS. HARRINGTON-MCBRIDE: I'm sorry, Joe, is that
10 you speaking?

11 MR. STSAUVER: That is me, I'm sorry.

12 MS. HARRINGTON-MCBRIDE: Great, that's okay.

13 MR. STSAUVER: They do enjoy some special
14 protection via the FCC in this case, so that's a special
15 difference I think that's important to call out for the
16 wireless folks.

17 MS. HARRINGTON-MCBRIDE: Okay. One of the
18 things that we've been hearing is that it may be less
19 possible for individuals who are viewing their Email on
20 a mobile device to utilize an opt-out function. My take
21 on this from what I've understood so far is that this
22 has to do primarily with the fact that the opt-out may
23 be in HTML as opposed to in text, and it may not be
24 possible therefore to access it from your mobile device.

25 Any information that you all have on that

1 potential problem?

2 MR. EDELMAN: This is Ben. The opt-out, one,
3 could be implemented in the HTML within the message
4 rather than in plain text, but, two, it would require
5 the user affirmatively to visit a web page, not just
6 parse out HTML but in fact go out and conduct an HTTP
7 get, get the page, fill out a form and submit it back.
8 That's a functionality that would not necessarily be
9 available on all mobile devices.

10 MS. HARRINGTON-MCBRIDE: Got it. Okay. Thank
11 you.

12 MR. STSAUVER: This is Joe. I would also like
13 to highlight the fact that opt-out, as a concept, causes
14 problems because simply the act of visiting a given web
15 site may result in a bit of malware being downloaded on
16 to a system, so the concept of having an opt-out
17 functioning is problematic for me for very practical
18 reasons.

19 MS. HARRINGTON-MCBRIDE: That's something we
20 would like to further explore as well. We have
21 certainly seen media reports about the theoretical
22 possibility of malware installation when one clicks on
23 an opt-out link.

24 We're wondering, even if it's anecdotal
25 evidence, what evidence you might have of the prevalence

1 of this practice, which would be anything that's
2 concrete would be very helpful for us.

3 MR. EDELMAN: This is Ben. I guess my
4 specialty, a dubious specialty such as it is, in the
5 past few months has been precisely in studying non-
6 consensual installations of Adware and Spyware,
7 generally through security hole exploits, and that
8 entire set of practices of such software being installed
9 non-consensually rather than by tricking a user into
10 granting a so-called consent through some kind of social
11 engineering. The non-consensual installations have
12 historically been rumored by the advertising industry to
13 be the thing of legend too; that is, it was previously
14 claimed that this alleged occurrence never in fact
15 occurred.

16 And that has now been thoroughly debunked I
17 suppose by myself because I have, in fact, posted screen
18 capture videos showing that occurring on some dozens of
19 occasions.

20 As to the link between opt-outs and such
21 installations, I haven't personally seen that. Then I
22 haven't been looking for it. It's actually something I
23 can readily do in the coming weeks. Of course there's a
24 fair amount of luck involved in happening to try one of
25 the right opt-outs at the right time to, in fact, get

1 that kind of installation.

2 MS. HARRINGTON-MCBRIDE: Ben, is there any
3 literature in the sort of the blog world about, It
4 happened to me here and that's how I know it happened,
5 because we thought that might be one way -- I appreciate
6 your concern about there being a needle in a haystack
7 searching. I don't know if there might be any sources
8 that you could recommend that we look at even on that,
9 where people might be talking about that.

10 MR. EDELMAN: Those sources are a reasonable
11 place to begin. They are a place where I would begin.
12 On the other hand, these infections are increasingly
13 stealthy. For example, a typical practice these days is
14 to install a typical stub via a security exploit, and
15 then go into some kind of a time delay, perhaps wait
16 until the user restarts his computer, perhaps wait until
17 the user restarts his computer for the fourth time or
18 wait seven days or what have you.

19 This means that the user may not know that the
20 computer has been infected until well after the
21 infection has incurred, making it quite a bit more
22 difficult to retrace the steps of what exactly gave rise
23 to the infection.

24 MS. HARRINGTON-MCBRIDE: Okay. That helps.

25 MR. EDELMAN: Victims are not so likely to know

1 these days exactly what it is that caused them to be
2 victimized, and that's part of the survival strategy of
3 those who seek to take advantage of them.

4 MS. HARRINGTON-MCBRIDE: Okay. Does anyone else
5 have any suggestions for ways we could find out the
6 prevalence of the installation of malware through
7 opt-out or any other inherent risks in opting out, any
8 way we could flesh that out?

9 MR. BELLOVIN: This is Steve. The usual
10 objection to opt-out is you're giving them confirmation
11 that there's a person at the end of that Email address,
12 and that's been the warning for a fair number of years.

13 MS. HARRINGTON-MCBRIDE: Okay.

14 MR. BELLOVIN: A confirmed live address is more
15 valuable or reportedly more valuable in the marketplace
16 for such things, and one that's just been synthesized or
17 gathered.

18 MR. EDELMAN: As to how you could opt-out, I
19 think there's a clear strategy of what you could do to
20 test the effectiveness or ineffectiveness of opt-out.
21 In particular, you would create a set of fresh randomly
22 generated Email aliases. You would provide those to
23 opt-out forms at various perhaps spammer sites, at least
24 commercial Emailer sites that purport to offer an
25 opt-out.

1 You would opt them out without them ever having
2 received a message, to be clear. You would opt them out
3 immediately, immediately at the creation of those
4 accounts and see what happened, see if those messages
5 ultimately receive -- see if those accounts ultimately
6 receive some messages.

7 It's not a difficult honey pot approach. It
8 seems like this should be pretty easy. It's the stuff
9 of blogs actually. This is something that any hobbyist
10 could do. You don't have to be the FTC to give this a
11 try, but you could too, and then see how many spams
12 those get.

13 I wouldn't be surprised if some of them do, and
14 that would be your smoking gun. That would prove in
15 fact that the opt-out is being affirmatively disregarded
16 and even used specifically contrary to its stated
17 purposes.

18 MR. BELLOVIN: This is Steve. You have to be a
19 little careful how you set that up to make sure you take
20 extremely improbable Email addresses because they're
21 doing total dictionary attacks across many different
22 ISPs and domains.

23 MR. EDELMAN: Yes, absolutely agreed.

24 MS. HARRINGTON-MCBRIDE: Okay.

25 MR. BELLOVIN: It's not something that a typical

1 hobbyist would get right I suspect.

2 MR. STSAUVER: This is Joe. The other point I
3 would like to make is even if you don't get hit with
4 malware when you visit an opt-out link, in other cases
5 you may be exposed to offensive content, so, for
6 example, you may go ahead and have attempted to opt-out
7 of one sort of scam or spam, but at the same time that
8 they're handling that opt-out, they may also feel free
9 to display additional ads at you.

10 So every impression is worth money, as it were,
11 even if it's apparently to folks who are trying very
12 hard not to receive that advertising.

13 MS. HARRINGTON-MCBRIDE: I'm a one note Charlie
14 here. Anything that you all might have on that that
15 would be concrete? So much of this world is sort of --
16 there are reports of lots of things, but it's very
17 helpful to us in making our report to Congress if we can
18 include even a small number of real examples. Screen
19 captures or things like that are very persuasive
20 evidence, and so if there's anything you have on the
21 idea that Joe has talked about, of being exposed to
22 further advertising content at the opt-out stage, that
23 would be interesting and useful.

24 MR. STSAUVER: We can provide that to you
25 offline.

1 MS. HARRINGTON-MCBRIDE: Sure, absolutely, and
2 I'll mention at the end of the call, but I'll certainly
3 say now, we're obviously doing this in a fairly tight
4 time frame, but to the extent that you have any
5 supplementary comments that you would like to make in
6 writing or orally beyond this call, the door is
7 certainly open for that.

8 The staff is looking to get a draft report done
9 in the very late summer, early fall, and so there's not
10 a huge amount of time left, but we certainly don't want
11 to say that as of noon today, we're done talking to you.
12 We would love to hear what you have to say if you have
13 some other ideas as time goes by.

14 One of the prevalent practices it seems to us
15 that certainly existed pre CAN-SPAM but which has taken
16 off to some degree since the passage of the Act is the
17 practice of filtering, and I wonder if there are any
18 thoughts that you have about how current, that is,
19 July 2005 versus December 2003, filtering practices may
20 affect the practicality and effectiveness of CAN-SPAM,
21 if at all.

22 MR. STSAUVER: This is Joe. One thing I've
23 noticed is it's become increasingly common for spammers
24 to go ahead and use multiple domains chained together,
25 so for example they may go ahead and spamvertise one

1 domain, and as soon as you visit that site, it will go
2 ahead and redirect to another site and potentially
3 further still to intermediary sites before getting to
4 the final site, and I believe that this is a reflection
5 of the increased usefulness of things called URI black
6 lists.

7 Probably the most common example of that is
8 SURBL, S U R B L, which is a black list run by Jeff
9 Chen, and what it does is rather than looking at the
10 source of the message, it looks at the spamvertised URL
11 and uses that as a filtering criteria.

12 MS. HARRINGTON-MCBRIDE: Okay.

13 MR. DAVIS: This is Mike Davis at the FTC. I
14 just wanted to interrupt and mention that if you have an
15 answer that may be a little forward looking and not only
16 covering the last 18, 19 months, but also if you're able
17 to look a little bit in your crystal ball and see
18 something happening just around the corner or even one
19 or two years out, we would love to welcome those
20 comments as well.

21 MS. HARRINGTON-MCBRIDE: Any other thoughts
22 about filtering and its impact on the effectiveness of
23 the Act or its ability to supplement the Act's
24 effectiveness or complement I guess the Act's
25 effectiveness?

1 MR. STSAUVER: This is Joe. It would also be
2 helpful to me to know if you're thinking about content
3 based filtering or if you're thinking about source based
4 filtering I guess?

5 MS. HARRINGTON-MCBRIDE: You know, I think we're
6 looking at all, the whole world of filtering and
7 everything that might have changed or become enhanced
8 since the passage of the Act.

9 What we're faced with is really trying to figure
10 out what was the state of the art at the time of the
11 passage of the Act, what's different now, and is any of
12 it different because of the Act or are any of the
13 changes making the Act potentially less effective. We
14 think that would be useful for us to be able to report
15 to Congress, so that if there are modifications in
16 whatever kind of technology, we can make them aware of
17 that.

18 MR. STSAUVER: I can flag one other example of a
19 change that's occurred, and that's the process of using
20 zombies has become much larger scale, so if you think
21 about a lot of the DNSBLs that have been deployed to
22 block traffic from zombies, typically they have a finite
23 site zone or filtering list that they can go ahead and
24 support, and I think in some cases you're actually
25 seeing so many zombies being created so rapidly, that

1 the effectiveness of those sorts of lists may become
2 less effective over time, simply because people have to
3 go ahead and continually purge old zombies from those
4 lists to make room for the new ones.

5 So if you go ahead and think about there being
6 perhaps two million entries in a typical zombie list
7 these days, I'm not sure it's going to scale to 10
8 million or 20 million or 50 million.

9 MR. BELLOVIN: There are techniques that one
10 could use to handle such large lists, this is Steve, but
11 they're harder to use because the infrastructure is not
12 really there to support it yet, so it is a more
13 problematic solution.

14 MR. DAVIS: Is that Steve?

15 MR. BELLOVIN: Yes, this is Steve. I was
16 thinking about large bloom filters, for example.

17 MS. HARRINGTON-MCBRIDE: I'm sorry, what kind of
18 filters?

19 MR. BELLOVIN: It's called a bloom filter, B L O
20 O M filters. It's a data structure technique. It's
21 about 35 years old, and it's got some very nice
22 properties. I won't go into the details of it right
23 now.

24 MS. HARRINGTON-MCBRIDE: Okay.

25 MR. BELLOVIN: One thing I will say, one thing

1 you can do in bloom filters is you can create -- if you
2 wanted a central opt-out list, you could create a list,
3 it would not actually be useful for -- it's not a list
4 of names. It's really a way to tell if the name is on
5 the list.

6 Now, someone could use it to validate the
7 existence of some names, but it's not the same as I can
8 just go read this list and copy the names off of it.

9 MS. HARRINGTON-MCBRIDE: Okay.

10 MR. BELLOVIN: It's a very space and time
11 efficient mechanism.

12 MR. STSAUVER: One other development that we
13 mentioned, this is Joe, is that Spam Assassin has really
14 become a de facto standard in a lot of the parts of the
15 market right now for content based filtering, and that's
16 good in the sense that it's a very good product, but at
17 the same time, it's also difficult because the spammers
18 then are able to go ahead and test potential messages
19 against Spam Assassin.

20 So they basically can go ahead and tailor a
21 potential message until it runs below the typical
22 threshold that's used. A lot of people, for example,
23 will run at a threshold of four, so because of that
24 standardization around one particular product, at least
25 in some market segments, filtering is becoming more

1 programmatic that's content based.

2 MR. BELLOVIN: This is Steve. There's another
3 trend that -- I won't call it a trend, something I've
4 seen a few instances of has been tailoring spam to
5 effectively attack carrier based anti-spam products.
6 There have been a few instances where the spam message
7 was carefully constructed to cause seriously accessed
8 SURBLs, in the analysis engine, taking advantage of
9 particular bugs or characteristics of those engines,
10 forcing the carriers to turn them off at least for a
11 short period of time.

12 MS. HARRINGTON-MCBRIDE: Huh.

13 MR. BELLOVIN: We haven't seen too much of that.
14 There have been a few instances of it.

15 MS. HARRINGTON-MCBRIDE: Are there any reports
16 of that in the media that we might be able to read
17 about?

18 MR. BELLOVIN: I saw at least one such report on
19 the NANOG mailing list a couple years ago. I can find
20 that and forward it to you.

21 MS. HARRINGTON-MCBRIDE: That would be great.
22 Thank you.

23 A recent study by the Pew Internet Organization
24 found that while volume of Email has increased since
25 their last study a year ago and since the passage of the

