FEDERAL TRADE COMMISSION

INDEX

COLLOQUY SESSION	PAGE
(LEAD BY:)	
MS. ROBBINS	4
MS. CHUA	56

FEDERAL TRADE COMMISSION

```
In the Matter of:                )
REPORT TO CONGRESS PURSUANT TO )
CAN-SPAM ACT.                    ) Matter No. P044405
-------------------------------)
```

WEDNESDAY

FEBRUARY 11, 2004

Room 249

Federal Trade Commission

600 Pennsylvania Ave., N.W.

Washington, D.C. 20580

The above-entitled matter came on for conference, pursuant to agreement at 2:15 p.m.

APPEARANCES:

ON BEHALF OF THE FEDERAL TRADE COMMISSION:

DANIEL SALSBURG
COLLEEN ROBBINS
SHERYL DREXLER
MICHELLE CHUA
KIM LUCAS
Federal Trade Commission
6th Street and Pennsylvania Avenue, N.W.
Washington, D.C. 20580-0000

PARTICIPANTS (VIA TELEPHONE):

JASON CATLETT, JunkBusters
CHRIS HOOFNAGLE, EPIC
PAULA BRUENING, Center for Democracy & Technology
CINDY COHN, Electronic Frontier Foundation

(IN PERSON):

CEDRIC LAURANT, EPIC

PROCEEDINGS

MS. ROBBINS: For purposes of this call, I'm going to go through a brief formality in the beginning. Today is February 11, 2004, and it's about 2:10 p.m. Eastern Standard Time. This call is being transcribed. I'm Colleen Robbins, an attorney with the Federal Trade Commission's Division of Marketing Practices.

I'm here with Dan Salsburg, Sheryl Drexler, Kim Lucas and Michelle Chua. We're all working on different reports as required by the CAN-SPAM Act that are due to Congress in the next few months.

Would the three of you on the phone introduce yourself for the court reporter and state your affiliations?

MS. COHN: I'm Cindy Cohn. I'm the Legal Director of the Electronic Frontier Foundation.

MS. BRUENING: Paula Bruening, Staff Counsel for the Center for Democracy and Technology.

MR. CATLETT: Jason Catlett, the President of Junkbusters Corp.

MS. ROBBINS: And again we have three other individuals who are not here at the moment, but will be joining us briefly.

Now, just to tell you why we're all here today, under Section 9 of the CAN-SPAM Act, Congress has asked the Federal Trade Commission to submit a plan and timetable for establishing a Do Not E-mail Registry. In addition, we also have to investigate the possibility of a possible reward system for identifying and locating spammers.

We need to submit these reports fairly soon, within the next six to nine months. We also need to include information under the report for the Do Not E-mail Registry regarding any practical, technical, security, privacy or enforceability concerns regarding a proposed National Do Not E-mail Registry.

The FTC is gathering information from various groups in a very short amount of time in order to assist us in drafting this report and the report on the reward system to Congress. As we said earlier, anything that's said during this conference today may be cited in the report to Congress.

I would like to start off by proposing one model for a National Do Not E-mail Registry. This model is similar to the Do Not Call model where consumers would register their e-mail addresses in a central registry, marketers would receive the list and scrub it so as not to send their e-mail to those on the registry.

I wanted to first get your ideas and thoughts on such a model.

MR. CATLETT: Should I jump in?

MS. ROBBINS: Sure.

MR. CATLETT: Sure. Junkbusters has loudly and for a long time opposed that. That model is impractical and counterproductive. There are many reasons I think that that won't work.

The primary obvious risk is that spammers will use it as a source of e-mail addresses, which has happened with such registries in the past.

Now, you can try to mitigate that risk by various means such as seeding, but the cat is already out of the bag there, and other than the method that's been proposed whereby lists are submitted for the -- submitted for well, scrubbing basically, but none of those is terribly practical.

And it also goes against the consumer's desire to keep their e-mail address private, which is what they've been told, that the paradox of having to make their e-mail address public in order to get some privacy, it really goes against all of the intuitions and desires of consumers.

I could also go on to the practical difficulties of the large number of e-mail addresses and the very fast changing nature of them. Twenty percent of them go stale in a year at least, but I think that this model is a nonstarter really.

Now, I would support a model that works with the domain name, but at the specific e-mail address level, I don't see that it's desirable or practical.

MR. SALSBURG: Jason, you referred to an experience in the past where addresses on the registry became available to spammers.

MR. CATLETT: Yes.

MR. SALSBURG: Could you elaborate on that?

MR. CATLETT: I'm trying to remember who it was. Various people have run -- I mean, there have been various scams involving Do Not E-mail Lists, which are really just used as -- were never really used for their intended purposes and were just used for harvesting, but I believe the ones I'm recalling that were legitimate and sincere were some by Rodney Joffe, Integrated Centergate Technologies I'm recalling, and another one run by Ram Avrahami, and I'm trying to remember which of those had that difficulty.

MR. SALSBURG: Could you spell the second name?

MR. CATLETT: Joffe is spelled J-O-F-F-E. Avrahami is spelled A-V-R-A-H-A-M-I from memory. But certainly if you go to the envelope world of direct marketing, the stealing of lists, mailing lists is a recurrent problem. You get a case documented every few months in DM News, and similarly with mooch lists and telephone fraud. You frequently have cases of lists being stolen by the criminals perpetrating telephone fraud.

So there's every reason to expect a similar outcome for e-mail lists, particularly when the list is extremely large.

MR. SALSBURG: You also mentioned seeding as a possible solution to protecting the security of a list, and you said that the problem with seeding is that the cat is already out of the bag. What did you mean by that?

MR. CATLETT: That's right, right. Well, once the list is compromised, assuming you have a model where the list is given to parties for scrubbing by themselves, then if you're giving a whole list to even one party who accidentally or deliberately sends it on to a spammer, then it's a impossible route to call that back.

They've got a copy of the list, and those problems have plagued, for example, people who have put their e-mail addresses as a contact for domain name registration who later found out that it's being harvested by spammers, and then some registrars allow you to make that information nonpublic, but it's already on CD-ROMs being sold by spammers for lists of spamming.

MR. SALSBURG: What would be the result for a consumer? How would they have to respond to this if their name became available?

MR. CATLETT: If their name was compromised and they were being spammed?

MR. SALSBURG: Right.

MR. CATLETT: Well, I think the expected emotional response of the consumer would be considerable disenchantment because they gave the government their e-mail address, which might otherwise have been secret and remained free of spam, and the result was that they actually got more spam and exactly the opposite of the intention.

So I think that would be a grave disappointment in the eyes of many consumers and would clearly be the conclusion of the party in having such a registry was a bad one because the risk was foreseeable.

MS. ROBBINS: Cindy or Paula, do either of you want to share your views?

MS. COHN: This is Cindy. I would we would certainly tend to agree with Jason to the extent that we do not think a model of the Do Not Spam List like the Do

Not Call List is a very workable one or a good idea, quite apart from the technical problems. I think Jason has done a good job with starting with the technical problems, starting to look at them.

I think there's a fundamental difference between telephone numbers and e-mail addresses that plays into this, which is that while telephone numbers really are not "born" private, they are to a certain extent either public or even if you have an unlisted number, pretty easily known.

E-mail addresses are "born" private. There is no international or national registry of e-mail addresses that exist. You're talking about creating one now, and so they start -- I think the owner of an e-mail address starts in a different location and has a different reasonable expectation of privacy in that information, and you can choose to give it out to people or not to give it out to people. You can choose to make it more public or less public in a way that you really don't have that flexibility with your phone number.

So by creating this list, I think you're going to fundamentally put people in a bit of a pickle where you're starting to create incentives for people to make public something that they could have kept private, and I think Jason's exactly right.

I mean, one of the things we have seen over and over again is the phenomenon -- of data leak. We call it Data Valdez at the Electronic Frontier Foundation. It's really hard to keep something secret even with the best intentions -- people are demanding that their data, personal data about folks, is kept secret. Even with the best of intentions, and of course there's no clear indication that every single governmental person who has access to this information is going to have the best of intentions all of the time, there will be leaks.

So the information is going to leak out, and I think as Jason indicated, once it leaks out, it's incredibly fluid. It's going to move. It's going to change. It's simply -- effectively once the information gets out, then what you've created is a situation where perhaps using the seeding technology, you'll be able to better track the people who are using it, but that's not really particularly helpful in the spam world because the people who are doing the spam move and change very, very often.

So once that information is out there, I think you're leaving the consumer with no choice but to change their e-mail address, and then I think they're going to be extremely hesitant to give it to the entity again.

So that's with all the best of intentions. I think that this is going to be an incredibly valuable database, and that the incentives for a rogue employee to try to get a copy or the master copy are going to be tremendous, and it's likely that that's going to happen at some point, again human nature being what it is, and whether it's an insider or whether it's just an extremely crafty spammer who figures out how to send another request to the database to try to verify names to recreate the list.

I think you'll see efforts to do that almost immediately, because again it's another difference between the phone situation I think and the e-mail situation where one of the things that is of a premium to spammers is to know the difference between e-mail addresses that don't have a person behind them and e-mail addresses that do. You're creating the big master list of real people, so to a certain extent I think that's counterproductive.

One of the things that's worked in the anti-spam community favor so far is the kind of technical reality that it's impossible to know whether there's a real person behind an e-mail address unless you test it. You're going to create the big master list, so we think that modeling something after the Do Not Call Registry, while it has appeal on a surface level, I think it really ignores a lot of the technical and kind of psychological differences between your phone number and your e-mail address.

MS. BRUENING: This is Paula. I think there's been some very valid points made here. What I would like to emphasize is the whole question of enforceability. Given certain limited resources and the kind of lists that we're talking about and what they would entail, the number of e-mail addresses, I think CDT's concern is that you would be creating something that at the end of the day would be extremely hard to enforce, would require probably more resources than we would anticipate sitting here having this conversation, and that when it doesn't work, what we've done is disappointed the consumer and possibly eroded the confidence they might have in the FTC's ability to stem the flow of spam and to control this problem.

I'm quite concerned that in trying to do something, which as Cindy said, on its surface looked like a very straightforward thing, in the end I think it would undermine the FTC and really aggravate consumers a great deal because something that makes sense in another venue, in their minds might make sense here too, but the outcome would be very, very different.

MS. ROBBINS: Does anyone else have any other thoughts on the enforceability issue?

MS. COHN: This is Cindy again. I think Paula is exactly right, and obviously there's kind of a constitutional underpinning to the question of whether the FTC or anybody can create a Do Not Spam List, and materially advancing the government's interest is the central prong of the constitutional test for regulations of commercial speech that isn't fraudulent.

I think that there is a really serious question about the ability of a Do Not Spam List to materially advance the government's interest, especially with the real negative things it's going to create, but I think that Paula's point about enforcement is incredibly important.

I think it's really, as a policy matter and as a legal matter, really important that the FTC doesn't spend a lot of energy on something that really isn't going to help the spam problem. The feel good measures are really not just a good idea in general, but I think it's especially problematic in this particular world.

MS. ROBBINS: Do you think that such a registry, if it included certain security precautions -- we've already talked about the seeding possibility -- but something that would include one-way hashes where there was a specific key that you would have to use to then convert encrypted e-mail addresses to actual e-mail addresses -- do you think that would make a difference and help make it more secure?

MR. CATLETT: It's Jason here. You could have a screen with one of the hashes that made it more difficult for spammers to extract the original e-mail addresses, but computationally in terms of time and space, I think it would be very difficult to get that working in a practical manner for anyone who was sincere about scrubbing their lists.

Let's not forget the fact that spamming is contrary to the acceptable use policies of all major ISPs, and no major company does that, so the people who are likely to use such a scheme, and I think that goes for almost any scrubbing scheme, are not using them anyway.

So I don't think it's finding a practical use particularly given --

MS. ROBBINS: I'm sorry, do you mean that they're sending permission-based e-mails?

MR. CATLETT: Yes, that's right, and they're not -- even if they're spamming -- major companies that are sending out bulk commercial e-mail are doing so generally with the permission of the recipient, and even if the recipient's address is on a Do Not E-mail List, they're still going to send it, and they have a right to send it given the specific agreement that they have with the consumer.

So I don't think that the -- I don't think that the registry generally would at an individual level, e-mail address level would provide a useful function, even if you were able to get through the technical difficulties.

I would also like to say something about enforcement unless you have something more on this.

MS. ROBBINS: That's fine. Go ahead.

MR. CATLETT: So enforcement is very important as Paula and Cindy said. You don't want to create an unsatisfiable expectation in the mind of the consumer, and unfortunately the FTC was dealt a very difficult hand by Congress.

Junkbusters and some other organizations strongly recommended the private right of action, which would have given a number of litigants proportional to the size of the spamming nuisance, but I don't see that the FTC can create a private right of action given the legislation that's being passed. It's plain that Congress did not intend that.

So what can you do in this case? I think it's still worth having a registry that allows domain name proponents to indicate that they don't want spam or to make that illegal.

I think one benefit there would be that the -- in the case of international spam, it may be easier for a plaintiff in a non-U.S. jurisdiction to prosecute under the laws of that jurisdiction for spamming a U.S. domain name if spamming was actually illegal in the U.S., and having a registry that allowed them to make their domains no-spam zones would effectively do that in the U.S.

So I think there's an enforcement benefit for some parties to having a domain name based opt-out registry much as I think that they opt out more and it does give a mechanism of changing the legal status of the spasm.

MR. SALSBURG: Let me first mention that Cedric Laurent from EPIC has joined us and is in the room with us now.

Jason, you mentioned possible one-way hashing schemes as a method of providing additional security to a registry.

MS. ROBBINS: I mentioned it.

MR. SALSBURG: Colleen mentioned it, and you commented on it.

MR. CATLETT: Yes.

MR. SALSBURG: Under such a scheme, wouldn't an e-mail marketer still need to have the ability to compare the hashes to their database of e-mails and would therefore know who was on the list and who's not?

MR. CATLETT: Do you want me to spend two minutes sketching the idea of one-way hashing?

MR. SALSBURG: Yes.

MR. CATLETT: Okay. So a hash is taken from the idea of a knife and some parsley or something you would chop up and hash and make unrecognizable. So what it is, it's a mathematical transformation that turns something familiar like catlett@junkbusters.com into a bunch of probably something like 64 random looking letters, but it's consistent in the sense that if you give it the same input in the same way, this is your key so that you can make the keys just like a combination lock number so that you can have different transformations.

So under such a scheme, instead of handing over a list of e-mail addresses, say a hundred million e-mail addresses, the FTC would hand over to a bulk e-mailing company a hundred million of these 56 letter hashes say, and what the spammer would do is suppose they want to spam catlett@junkbusters.com, they apply the same hashing function which is a specified piece of software to the address that they want to spam, say catlett@junkbusters.com and come up with such a big number after applying their key also and then they compare it with the list.

Obviously they have to have a database and function that allows them to efficiently look up one in a hundred million addresses, and then they say, "Uh-huh, catlett@junkbusters.com was on this list," but having been hashed, the problem is that they can't know the advantages, that they can't automatically get that list and use it for spamming. They could use dictionary attacks, like they could say "Well, let's get junk41@aol.com as an e-mail address, and see if it is," but again they can use the dictionary attack by directly going to AOL and testing for -- using the protocol for whether junk41@aol.com is an effective e-mail address.

It makes it slightly easy for them because AOL will cut off that kind of behavior with a bit of spamming. One other technical thing, you can make the hash key different for different parties so that provides a kind of seeding, but the whole idea is extremely cumbersome in terms of the amount of data you're moving around, the computations that have to be performed.

And as I said, you're solving a problem that legitimate parties don't have anyway, so I don't think that's a meritorious idea.

MS. COHN: This is Cindy. Jason has done a great job of describing hash functions and how they work. I think the fundamental thing that's important to remember about them and how they would apply here is that at the end of the day, the spammer still has to get the information about whether this e-mail address is on the list or not, and that information -- if you don't give them that information, then they can't sanitize their list, but the minute they have that information, then they know which of the names on their list are good names and which of the names on their list are not necessarily good names.

There's no way that a hash function -- hash functions are designed to mathematically do several discrete things. One of the things they're not designed really to do is to have one end of the discussion be able to hide something from the other end of the discussion.

MR. CATLETT: Right, right.

MS. COHN: That's what you really -- I think they're trying to be applied in this particular context to do that and they don't. They're really good at stopping someone in the middle trying to figure out what information these two people are exchanging, and they're pretty good at making sure that the information that's being exchanged doesn't get changed in the middle.

So if I tell you that this is a message that Jason wrote and then I hash it and you check the hash and if the hash number would be different if I've altered Jason message from the original one, it's good for that.

But there's no way that you can apply a hash function solution or suggestion here that would do I think what people are hoping it would do, which is make sure that the spammer doesn't actually know which e-mail addresses are on the list so they can do bad things with it because you have to let the spammer know which e-mail addresses are on the list so they can do the thing you want them to do which is sanitize it.

So I think that -- I think that to a certain extent it will stop the wholesale taking of the database and then selling it, but I think all you'll do is take it up one level, and spammers are going to start doing -- they'll start selling the lists of the hashes or the list of the things that we have checked with the hash and all of these people are all people because they're all on the FTC Do Not Spam List, there you go, that's added value for you, you know that these people exist.

There's no way to stop that, which I think is the fundamental criticism of the Do Not E-mail List that you've heard from a lot of people -- that you're creating another list of good e-mail addresses. There's nothing about a hash function solution that would change that. I think I'm rambling a bit.

MR. CATLETT: No, no. I think Cindy has made an important point that just because it uses encryption, and it does use cryptographic techniques, doesn't mean that the information is secure from the party of about whom you had the most suspicion.

MS. COHN: Right. That's right. It does stop third parties from finding out information, but in this particular sense, the suspect party (that's the threat model, to use the term that security people use), is the person you're actually giving the information to. A hash function can't help you protect against those people.

MS. ROBBINS: Just to bring Cedric up to speed, we were asking them to comment on modeling a Do Not E-mail Registry after the Do Not Call Registry. And so do you have any thoughts just before we move on on that?

MR. LAURANT: I was about to talk in general about the OECD workshop on spam that was held in Brussels recently in which no one really tackled the issue, and as well as about the recent Communication from the European Commission on spam that does not address the issue at all either. This is because the European Directive on Privacy and Electronic Communications establishes the opt-in principle as a general rule for all e-mails that are sent to individuals, while the idea of a Do Not Spam List starts with the assumption that consumers usually prefer the opt-out approach.

MR. HOOFNAGLE: Hi, everyone. This is Chris Hoofnagle. My previous meeting ran late, so I apologize for being late, for joining in late.

MR. SALSBURG: Welcome Chris.

MS. ROBBINS: Chris, just so you know, this conversation is being transcribed. There's a court reporter here, so you will need to say your name before you speak.

MR. HOOFNAGLE: Thank you.

MS. ROBBINS: Chris, just to give you an opportunity to comment as well before we move on, what we have been talking about is the possibility of modeling a National Do Not E-mail Registry on the National Do Not Call Registry model. Do you have any thoughts on that?

MR. HOOFNAGLE: Yes, I do. I do think that there are serious technical issues with creating a Do Not E-mail address list that is similar to the Do Not Call List in that it has an actual list of phone numbers. It's been my impression that it might be a friendlier approach to allow people to enroll by domain names where possible. That was my primary concern about the Do Not Call model.

MS. ROBBINS: Do you have any thoughts on what the problems are with the model in terms of enforceability or security or privacy concerns?

MR. HOOFNAGLE: Well, with all three. I think that you have the problem of harvesting or improper use of the list. You have the privacy problems of transmitting the list of all that personally identifiable information to the government. It seems like it's a friendlier approach to allow people to opt-out based on a domain name rather than in the individual e-mail address, particularly because of the privacy concerns than the problem of the list actually being used for the spam.

I know that the direct marketers can employ certain techniques to detect whether or not someone is using the list for harvesting, but I think that works really well in the telemarketing world or in the direct mail world.

I'm unsure of how well it will work in the spam world.

MS. DREXLER: This is Sheryl Drexler of the FTC. I hear both Jason and Chris talking about a domain opt-out and I'm wondering how you envision permission based marketing, your newsletters for example, to still reach inboxes if you had a domain wide opt-out?

MR. CATLETT: Let me speak to that. I think we have an obvious precedent with Do Not Call and Do Not Mail systems, which simply state that a specific request or round of permission by a consumer overrides the general election.

So if I put my name on a Do Not E-mail List or if I put my phone number on a Do Not Call List, I can still go to Lands End and say," Please e-mail me your catalog or please call me every time that a new color of sweater comes out so that I can order it immediately." That election overrides the general election, and I see absolutely no difficultly with that.

MS. DREXLER: How about technically? How would you envision that working? Would you see the domain opt-out scrubbing occur on the spammer's end or from the ISP's end and how would that work if I was a person who registered on the List?

MR. CATLETT: The ISPs should not block all commercial e-mails based on the election of a domain name to be a no spam zone. It should be the marketer, the legitimate -- the legitimate marketer gets individual permission overriding the domain name and the spammer doesn't bother to, and spams the addresses in that domain regardless and risks the consequence of prosecution.

MS. DREXLER: Does anyone else have any thoughts on that?

MS. COHN: This is not an idea that I have thought about much, so I guess I would reserve my thinking about it. So not at the moment, but I may as I think about it more.

MR. SALSBURG: This is Dan. Let me ask you this question: Would there be any difference in the enforceability of a domain wide opt-out list versus a list of actual addresses?

MR. CATLETT: Let me make a comment on that. From the point of view of the question of whether a particular domain was off bounds versus particular e-mail addresses off bounds, it would be easy to implement a system that makes the domain information available at very low cost in a ubiquitous fashion because we already have -- well, for two reasons.

One is the list of domain names is so much smaller that you could fit it on a USB/memory card. There are only hundreds of thousands of domain names and they're fairly short. So that would -- in terms of distributing the information, that would be much easier. It would be much lesser burdensome on anyone who really wanted to comply with that opt-out.

It would also be a much more economical for the FTC to be dealing with that level of information, and to Cindy's point about the fact that phone numbers are already sitting ducks whereas e-mail addresses are not, domain names are already sitting ducks because of the domain name system. It's technically necessary that at least second level domains such as aol.com be publicly accessible, so it's much more analogous using her reasoning to the telephone number case.

It would also be simple to or at least a simple matter of programming that part, but possibly more difficult engineering in terms of scale, to modify the domain name system to include the information about whether such an election has been made which would effectively provide a Do Not Spam database, which is distributed entirely efficient in the same manner that the domain information and a load of other information is provided by the DNS.

Incidentally, as an aside, the man who wrote the DNS system, Paul Vixie, is also one of the most hard working anti-spammers, so I think that he would have some easy technical support in the community.

So coming back to Dan's question of would it be easy for enforcement, I think it would be much easier for a prosecutor to show that the spammer -- an address was off bounds at a certain time, and that the spammer could have found that information and that there was no likelihood of a technical failure, that meant that although they were in good faith trying to purge the list, they made a mistake and so forth.

With a domain name prohibition, that's obviously a very simple thing to do, to get the domain name right. If you go to a complex encryption system where you have these hashes and you're doing hundreds of millions of e-mail addresses, a defendant could more plausibly and easily argue that they made a sincere mistake, and this whole thing was a terrible misunderstanding, et cetera, et cetera.

MS. ROBBINS: What about in terms of actually identifying the spammer though? Would you think there was a difference in enforceability in that respect?

MR. CATLETT: I don't see that. I don't think that would be the case. I don't think so.

MR. SALSBURG: In other words, let me follow up on that. If a spammer ignored a registry of addresses, and just never bothered to even register and get a copy of the list but then sent spam, that would be as likely to happen with a domain registry?

MR. CATLETT: Well, I don't know because you're asking a question there about a spammer view, which is difficult to predict. One obvious effect is the FTC in its implementation of the Do Not Call List has a mechanism where you can follow the money and see who bought the list and who didn't even bother to do the list.

Now, the FTC could implement a domain based registry whereby spammers paid to get the list, but I don't think that would be the most desirable implementation. As I said, I think the more cheap and efficient and ubiquitous system would be to have something analogous to what was built into Paul Vixie's DNS, and in that case the FTC would not know whether the list -- the spammer had attempted to get it because they had the financial record that that entity purchased the list.

So maybe that's a difference that you may consider.

MR. SALSBURG: Jason, can you spell Paul Vixie's last name?

MR. CATLETT: V-I-X-I-E.

MR. SALSBURG: Also you mentioned that there are probably hundreds of thousands of domain names versus the much larger number of e-mail addresses.

MR. CATLETT: Yes, hundreds of millions.

MR. SALSBURG: Does anyone on the telephone know where we can get statistics on both those figures?

MS. COHN: Yes, it's called VeriSign.

MR. SALSBURG: For the number of domains. How about for the number of e-mail addresses?

MR. CATLETT: I didn't get the question.

MS. COHN: I don't know of anybody who has a hard -- VeriSign ultimately knows how many domains are registered, at least in the ones that it controls. You're not going to have some of the foreign lists, but anybody that has a root server should be able to do a count of how many domains they've at least handled.

In terms of e-mail addresses, I think that's like chasing the sunset because that's a big changing number, and I don't think there's any -- there's certainly nothing I'm aware of that any of the technology that lets you create e-mail addresses for people that would ever report back to anybody about how many it is.

MR. CATLETT: Yeah, you're never going to get an accurate number, but you can do a back of the envelope calculation that is going to get you to within a factor of five I think. You take the online population of the world and say 200,000,000 -- 200 million, and then you estimate that on average each of them might have three e-mail addresses, so you are getting up towards a billion e-mail addresses.

And that number might be up by a factor of five one way or the other, but Senator -- I can't remember who said it -- one of the U.S. senators -- a billion, here a billion there, pretty soon you're talking big money.

MS. COHN: This is Cindy, Jason is unequivocally right. There are fewer domain names than there are addresses by orders of magnitude. What that exact number is, I have no idea, and I think Jason is right about how you begin to go through doing it, but I don't think there's any serious dispute that the number is smaller, and quite a bit smaller.

MR. SALSBURG: The reason we've asked this question is to get a sense of database management, if there was registry.

MS. COHN: It's still going to be pretty big with domain names, I think, especially as I said lots of folks are anticipating at some point ICANN is going to loosen up on the creation of new domains, top level domains. They're going to -- at some point that's going to grow I think at least. Who knows.

Who knows if they keep on moving, and even in the .com and .net and .org, it's kind of a general world but the numbers are -- it's still going to be a good size number.

MR. HOOFNAGLE: I think we also have the difficulty of calculating that number, that someone could have a wild card e-mail address, so for instance, I could register epic.org and put a wild card on my mail server so that any e-mail, any string of letters or numbers before epic.org landed in a mailbox, I mean, that could be many thousands of e-mail addresses -- well, many millions of e-mail addresses.

MS. COHN: This is Cindy again. I think that in terms of enforcement, that there is some enforcement fall out because it's a smaller database, and I think Jason's right about that, but I think that the fundamental enforcement problems are pretty much the same as to the two kinds of lists in that most spammers aren't following the law anyway.

Most of the stuff that CAN-SPAM made illegal was already illegal, so which is one of the kind of observations about the law that we have at EFF, so it's not clear to us how more law is going to change the numbers significantly. There are already people who are working hard to hide who they are and where they are, and there's nothing about this list that changes that.

I guess as I'm thinking about the domain name thing again, I don't really have a position on it. I do think there's a level of complexity if it is the case that the domain can sign on, but then individual e-mail address owners opt-out in specific instances, I think there's a level of complexity to try to figure out, from the senders's perspective, when it's okay and when it's not okay.

Again that may be a level of complexity that we don't mind putting on the sender of the e-mail. I think in terms of having people have to pay to get this information, it's not only counterproductive, but I think they're constitutional problems. We're talking about speech here, and there's a limit to how much the government can burden it, and I think instituting a payment scheme to be able to send commercial messages, the government tax on commercial messages would have some serious constitutional issues raised on it almost immediately.

MS. BRUENING: This is Paula, and I would like to second what Cindy has just said, about there are speech issues working all over the place in spam legislation, and it's an extremely delicate balance that we're trying to strike here, and I agree that as soon as you start charging people, it just sends up red flags all over the place.

So while I haven't looked closely at the domain name approach to this, I think we have to be really careful about charging. When money starts coming into play and anything that's creating any sort of potential bottleneck where the burden becomes sufficiently great, there's going to be push back on that.

MR. CATLETT: Yeah. Let me just add a comment on the costing. Do Not E-mail database at the level of domain names is a serious engineering project and would require at least millions of dollars and my guess probably tens of millions of dollars, but in terms of total cost over several years running into hundreds of millions of dollars, and that's a lot of money for something that's not going to work and do anything useful at all, whereas at the level of domain names, it's a really very minor, comparably minor cost.

If it's implemented through the DNS, then all those costs would be sunk in general into the infrastructure costs, and they would be one billionth of the cost that the Internet pays for carrying spam around every day.

Even if the FTC implemented a list that could be downloaded off the FTC's web site, that could be done for a very small amount of money for some time would be my guess.

MS. COHN: Jason, I know the FTC is supposed to be asking us questions, but I'm curious about the DNS implementation. Can you explain that a little bit more?

MR. CATLETT: Sure. The DNS is a system which basically you give it a domain name like ftc.gov or www.ftc.gov and it gives you an IP address which is the numeric number of the computer running the web server so that your browser can say, "Go get the FTC's homepage."

Now, in order to do that transformation, there's not a central database that says every domain name is www.such and such. It's a distributed system whereby the DNS software runs on a lot of computers, and requests are made as they're needed because a lot of people ask for www.cnn.com, and those -- the information is held for a certain time because things have to change -- they have to change locally, and it's computationally a very efficient system.

Now, it doesn't just handle web site addresses, for example. It also handles information such as mail, where do -- where do I deliver my mail, and the mail server information for www.ftc.gov may be very different to the mail sorter information, so it's a web server information for ftc.gov.

So it would be -- technically it's feasible and I think sociologically very plausible to add to that the software or mechanism to include a simple election about the domain name.

Now, another way it could be implemented is using the information that the registrars provide. That's a completely different mechanism. When you register a domain name, the registrar maintains that information such as the technical contact and the administrative contact and certain other information which can be provided publicly to anyone that the registrar chooses through a "Whois" inquiry.

And we've actually complained along with many other privacy organizations that too much information is -- total information is provided too easily with Whois information. But that would be another place where it would be easy to add a field of information which simply says, "This domain has elected to be -- to not receive spam."

MS. COHN: I'm sorry to interrupt. So then the way that this would play out is if you're wanting to send out non-commercial e-mail messages to a domain, the first thing you would do is check if there's any DNS, your local DNS database or the --

MR. CATLETT: Or the Whois database.

MS. COHN: Then you have to go back and say, "Is the individual I'm going to send this to, even though they're in this domain, did they tell me separately that they didn't --"

MR. CATLETT: Correct.

MS. COHN: That was the piece that I wasn't sure of.

MR. CATLETT: Let's not forget the way it works for legitimate marketers now is they're only sending out e-mails to people who requested it, and if they're doing it right, which most of the ones that keep doing it are doing it, they have records of when the person signed up and the IP address that they come through because they do get complaints, people saying, "Well, I didn't sign up for your list" so they can come back and say, "Yes, you did, here's the details," so marketers who have permission would not be burdened even with checking because they have the individual consent.

Where I see the advantage of this for a domain name based registry is that it provides businesses and many individuals with a means of saying that they don't want spam. You might ask what good does that do right now because only the law enforcement can enforce this law, and the answer may make it easier in that case, but we have to look forward to an improvement in the law. I think it will quickly prove unsatisfactory.

And eventually the U.S. and every other country in the world will go to an opt-in for e-mail, so it may be that for a period we just have an opt-out law in the U.S. with domain name opt-out, and if we could get the law modified so that there's a private right of action plus a domain name opt-out, that would be a great improvement and would allow the problem to be mitigated.

So even if the FTC has concerns that it would not have a great deal of resources to enforce a domain named base or opt-out, I think it's still a worthy investment to make on the assumption that private right of action or other enforcement resources may be certainly strengthening the enforcement under the current statutes, and it's good to get that infrastructure going early so that we can benefit from the stronger enforcement when it's available.

MR. SALSBURG: Would adding a no spam tag to DNS information require a change to Internet protocols?

MR. CATLETT: Well, you've got to -- the term Internet protocol is a technical term which has to do with the very low level packet, packet level, so let me just answer your question without answering -- with avoiding that term Internet protocol, so I'll rephrase your question, which is: How much of the public infrastructure would a domain name based opt-out system require?

The answer is you could go do it without any change to the public infrastructure if you wanted to. The FTC could simply collect domain names and publish them as a file that was downloadable, and for some time that would be practical because you would only have a text file of in the order of megabytes, not hundreds of gigabites as the individual address list would be.

So you could do it that way, but I think in the longer term, a more desirable method would be to do it through the Whois on the DNS databases, which would require changes by other parties, and there's a plausible mechanism for propagating such changes. Those sort of the changes historically have taken place frequently, and the problem is motivating the parties, so I think that's very feasible and to do that with the simple system of a text file, downloaded text file in the interim.

MS. ROBBINS: Any other thoughts on the domain wide opt-out model before I move on to another proposal?

MS. COHN: I would just say that I think that Jason is certainly right about the first option that he gave, that if you guys just the list of names available, that wouldn't make any infrastructure changes. I guess I'm a bit less optimistic that it would not be disruptive or easy to convince the folks involved in the domain name system, and Paul is not God over there, to implement it.

I'm not saying it wouldn't be possible, but I'm not quite just saying that it would be all that easy, and certainly if you're going to implement it to the database through the Whois database, I think there will be some resistance. There's a lot of discussion going on about the Whois database and -- who should have access to it, and so I again think that it may not be quite so simple to change the technological level as Jason has outlined.

But that doesn't mean it's impossible. I'm just a little more skeptical perhaps.

MR. CATLETT: Yes. Certainly I wasn't saying it's a slam dunk, and the phrase "simple matter of programming" is 100 percent ironic in the technical community, but changes of such magnitude do get made when the motivation is sufficient.

So I think we have a good shot at that over the longer term.

MS. ROBBINS: Before we move completely away from this model, one other possible format could be that the addresses entered into the Registry would be provided to an unsolicited commercial e-mail forwarding service approved by the Commission. E-mail marketers would be required to send all unsolicited commercial e-mail to this forwarding service, which would then forward only those e-mails addressed to recipients who had not signed up for the Commission's Registry.

MR. CATLETT: May I ask, and who would pay for the bandwidth cost of this forwarding?

MS. ROBBINS: That's why we're asking your thoughts on this.

MR. CATLETT: I don't want to be funny.

MS. COHN: This is Cindy. I think that's a horrible idea from a policy perspective as it is undoable from a technical perspective. I can't say which part of that is worse.

From a technological position, I think the bandwidth costs are tremendous. The reason that the Internet has been the amazing mechanism for growth and development of things is because it is decentralized. It's because there's no bottleneck. There's a choke point that you have to go through in order to get your messages from one place to another, whether it's e-mail or your web sites or whatever.

And decentralization has been the engine, and what you're talking about is instituting centralizing, at least on some e-mail, for a tremendous percentage of what happens online. We haven't even touched on some of the structural issues or what does commercial versus non-commercial mean and how are you guys going to define it, which is going to determine the breadth of what gets impacted here.

But by any measure, it's a huge amount of information that is going to fall under your category of what gets regulated here, so you're basically instituting some form of centralization on something that its greatest strength is its decentralization.

I think as a policy matter, it is such a bad idea to turn the Internet or even a piece of it -- and turn it into a centralized system. It is the biggest step backwards that I can imagine for the current technology.

And I don't actually have to make the policy argument because I think technologically it's not going to work anyway. You're not going to be able to do the kind of checking you need to do and have the e-mail system work even remotely like it would know.

MR. CATLETT: I think Cindy has really understated this case here.

MS. BRUENING: This is Paula. I think Cindy took the words out of my mouth.

MS. COHN: Sorry.

MS. BRUENING: I think it just is getting really far away from what makes the Internet and what makes the e-mail system such a powerful medium for speech and for commerce and for all those other good things.

I think the idea of a bottleneck is the worst direction we could go in, and I know that there are a lot of businesses springing up that are coming up with field programs and ways to review e-mail, and our sense is if that's the way the marketplace is going, clearly we should experiment with those, but to take the leap and bring that whole function to government I think is a very bad move.

MS. COHN: I also think the constitutional problems are really immediate. The government is suddenly the great arbiter of whether the mail gets delivered or not based on a system which is allegedly non-content based, but you can see how easily it can go in a different direction.

We already have problems with some of the technologies that are doing spam filtering privately are being accused, and there's some good evidence, that they're being gamed to try to stop certain messages based upon content rather than based upon some sort of objective measure of whether it's spam or not.

And setting aside the question whether commercial or non-commercial content, we're talking about people that are trying to stop political messages that they don't like. Imagine the opportunities to do that if the government was the great arbiter and that that would happen. I think the constitutional problems are tremendous here quite apart from the other tiny problems.

MS. ROBBINS: Okay. Well, let's move on to a fourth possible proposal for a registry format. This is actually taking consumers completely out of the picture. E-mail marketers would register with the Commission and provide information regarding their ownership or location, and they would be assigned a registration number, and that registration number would have to be inserted into all their unsolicited commercial e-mails.

Prior to sending any unsolicited commercial e-mail, as part of the registration process, the e-mail marketer would be required to provide the Commission with their IP addresses from which the mail would be sent.

Then the ISPs would have access to a database of these registration numbers and IP addresses. When mail would go through the ISP, the ISPs could adjust their filters to check the registration number with the corresponding IP addresses, and if they didn't match, then the mail would not go through. That would be an attempt to authenticate who was actually sending the e-mail.

MS. COHN: Is the main -- the government is going to maintain a list of the registered speakers?

MS. ROBBINS: Registered marketers that are sending unsolicited commercial e-mails.

MR. HOOFNAGLE: I think the use of unsolicited commercial e-mail is being a bit overstated here. Businesses generally have to register in the United States when they form corporations. I think we shouldn't overstate the case as if the spammers should have anonymity in their business practices when business law does not allow that.

MS. ROBBINS: Does anyone have any other thoughts on that type of model?

MR. CATLETT: I'm just trying to relate it to the statute. The statute is an opt-out model, and you're saying that in order to comply with opt-out, I have to register my IP addresses, so suppose I'm a mom and pop operation and I've got a little newsletter from my wine business or something like that. Now, it's all opt-in. Do I now have to go to the FTC and register my address in order to keep sending to the 30 people who get my wine recommendations each week? Is that the proposal?

MR. SALSBURG: Let's stick with the scenario where you have to register as a marketer of unsolicited commercial e-mail.

MR. CATLETT: Okay. So if it's all permission based, then I don't have to register, and if I'm sending unsolicited mail because of the possibility of sending to someone who's on the Do Not Call -- Do Not E-mail List, I have to register, and then what else happens?

MR. SALSBURG: And you provide your IP addresses.

MR. CATLETT: Provide my IP addresses.

MR. SALSBURG: And so that --

MR. CATLETT: What if it's a dynamic IP address? I'm a mom and pop operation. Every time I dial up it's a different address.

MR. SALSBURG: Let's change the fact pattern a bit. What if such a scenario were limited to bulk e-mailers who basically have static IP addresses?

MR. CATLETT: Well, plausibly?

MS. COHN: That's not a very safe assumption.

MR. SALSBURG: Let's assume then that a bulk e-mailer has the capacity to contact the FTC and inform it what dynamic IP address it is currently using right before it sends it.

MR. CATLETT: Spamming. Let's assume that we have real time updating of the address, and then what happens?

MS. ROBBINS: Once the mail goes into an ISPs' system and through their filter, the ISPs would have access to the database and can determine whether or not the registration number matches the IP address.

MR. CATLETT: Okay. So basically what you're introducing here is a tracking system for commercial e-mail. Where does the opt-out come in? It seems to me you're trying to do something else. It seems to me the proposal is a tracking system, not a scrubbing system.

MR. SALSBURG: Rather than characterizing, let's talk about whether there are any merits to stopping the spam problem or not. Let me give you a little background that might help the discussion along. ISPs are already engaged in an approach where they have whitelists based on e-mail marketers that provide their IP addresses. If they're on the whitelist, the mail goes through. If they're not, it doesn't go through or it gets reviewed at a different level by the filters.

MR. CATLETT: Sure.

MR. SALSBURG: In essence this would be federalizing that process, so if you're an e-mail marketer, rather than having to be whitelisted by the 700 ISPs in the country, you would be whitelisted by the government.

MR. CATLETT: I have to think about this one.

MS. COHN: I would have to think about it too.

MR. SALSBURG: Is there anybody that wouldn't have to think about it?

MR. LAURANT: So it would apply to spammers based in the U.S. sending e-mails to customers and consumers based in the U.S.?

MR. SALSBURG: That is a very good question, and that's a question that would go to any of these models. What would be the extraterritorial effects of any of these models? We can talk about that now.

Let's take the other models we've discussed, the registry of e-mail addresses or the opt-out registry for domains. Should this apply to e-mail marketers from abroad who are trying to send spam to Americans, and what kind of limitations, if you had these databases set up, could you put in place to ensure that the only people that could register were Americans?

MR. CATLETT: Let me state, I think you should allow any domain name, no matter where it's registered and no matter where the business entity or the individual owing the domain is established, and you might ask why -- you might ask why.

I think the purpose is to allow U.S. law to be brought in where it's applicable. For example, if the sender is established in the U.S. or obviously is availing themselves of U.S. markets, then it seems to me legitimate to apply U.S. law, even if it is sending to a non-U.S. entity, if the non-U.S. entity has elected to avail itself of the Do Not Call option.

So that's the way I would like it to be. I'll leave it to you lawyers to see to what extent you could get that to work.

MS. ROBBINS: Anyone else have thoughts on that?

MR. HOOFNAGLE: This is really a hard issue. You're dealing with companies that are soliciting business amongst American consumers. Is it not presumed that American consumer protection law will protect the Americans, the American subscribers regardless of where the domain is actually located?

MR. SALSBURG: No, I think you're right about that. Let's change the question slightly, to be: How could the FTC enforce any sort of registry requirement against a foreign sender of spam?

MR. HOOFNAGLE: That's a really good question. Although there are a lot of reports out there about spam, I'm still under the impression that most of the spam actually advertises American products. I think also it's worth -- and therefore there's ultimately American companies involved.

I think it's also worth noting that no amount of effort is going to eliminate all spam, and so it's worth the exercise even if we don't get international -- or even if there's some percentage of international spam that will escape enforcement efforts.

MR. CATLETT: Yeah. Could I add here? I think that enforcement authorities in other countries will take some notice of whether the spamming was illegal in its destination. I think that certainly UK law has this doctrine that if you conspire in the UK to do something, that although it may not be illegal in the UK, it's illegal outside the UK where it's to be performed, then UK enforcement can still go after the perpetrator in the UK.

And I would have to look at the specific details of that with an expert, but I think it could do the world benefit enforcement authorities oversee outside of the U.S. if the act was really illegal in the U.S., so and making it easier to opt-out all domains and making it absolutely clear that spamming was illegal may help enforcement authorities outside the U.S.

MS. COHN: This is Cindy. I think that the U.S. -- I'm not a complete expert in the United States jurisdiction, and they actually vary a bit from state to state depending on long arm statutes and things like that, so I think it's hard to be definitive, but it's generally not the case that the United States can reach outside of the U.S. for purposes of enforcing its laws, except in very pretty specific exceptions to the rule.

I'm not sure this would fit into any of them from -- I guess you might create a whole new one, but I think that's worrisome, so I would worry a bit about the United States appearing to think that it can be the world's spam policeman or being perceived that way.

I don't think that's a really very wise course. I think Jason makes a valid point, that simply indicating and making it clear that something was illegal in the United States could be helpful with people trying to do enforcement efforts abroad, but I think that's different than saying that we can actually -- to take on for ourselves the idea of policing the world of spam problems, even as the people who aren't in the United States aren't subject to our laws and certainly jurisdictions -- simply because you're sending e-mail to a person in the United States does not confer general jurisdiction or specific jurisdiction generally on that person for purposes of U.S. laws.

MS. ROBBINS: Do any --

MS. COHN: Go ahead.

MS. ROBBINS: Do any of you think --

MS. COHN: Let me just be clear on this. Cindy, again. The reason it shouldn't is perhaps is a little more indirect. It's because I don't want to be subject to the laws of Saudi Arabia because I send an e-mail there. You have to remember how reciprocity tends to work in the international arena. I don't think the U.S. wants to start down that slippery slope with the rest of the world because we have a legal system on free speech that's interest is much more protective, and I think we want to ensure that Americans have that protection even if they happen to be sending a message to someone in a country that is not as protective of speech rights as we are.

MS. ROBBINS: Does anyone think that any of these models are workable in any fashion, and if not, does anyone have any other ideas for other potential models for a Registry?

MR. SALSBURG: By workable we mean not only is it something that could be implemented, but it would have a significant impact on the amount of spam that consumers are receiving.

MR. CATLETT: Well, let me restate what I said earlier, I think the only practicable model is the domain name level one. Whether it will have an effect depends on enforcement, and at the current level of government enforcement, I don't think that that's going to be significant.

However, if the federal law was subsequently modified to have a private right of action or to allow the States to introduce a private right of action, then the domain -- and we have the domain name registration in place, then that could have a significant -- could have a significant effect, and it may have a beneficial effect in other jurisdictions where private right of action is available. I don't know.

So to summarize, I think that only the domain name level is workable. It would not likely have a significant effect with the current enforcement regime, although it may facilitate some other cases and make enforcement more efficient, which is important given the very limited resources that law enforcement devotes to it.

But in the longer term, it may be very useful to have that infrastructure built and available.

MR. HOOFNAGLE: I think we may agree with Jason completely there, but I think it's also worth analyzing this problem in seeing it as an opportunity for the agency to reevaluate its position on opt-in and opt-out.

When we were originally contacted by the agency, when it decided to enter the spam debate more fully, the agency official indicated they were going to start from the opt-out paradigm, but as we go through these exercises of implementation in fairness to the consumers, in the implications of opt-out, I do think it is a -- it's providing more and more ammunition for the agency to reject that approach and move towards opt-in generally as a better solution to protect communications privacy.

MR. CATLETT: Could I add that the domain name level opt-out will become a kind of opt-in in the sense that there is a significant amount of enforcement applied or if there's a private right of action available, almost everybody who is awake will make the election of their domain name to opt-out of spam.
For one thing, if it has even a slight effect, it will save business a significant amount of money on their bandwidth. Therefore they will do it.

So in terms of constitutional qualms, some legislatures will be less hesitant to go for an approach that allows a domain level opt-out than to impose opt-in, which I think they should still impose opt-in, but the reality is that if some of them have those qualms.

So I think to Chris's point, if the FTC feels unable at the moment to recommend an opt-in approach, at least I think it could consider this thought of opt-in or of saying allow domain name opt-out.

MS. COHN: This is Cindy. I think that there is a central registry plan that -- I haven't thought about Jason's plan enough to comment on that, so let me set that aside for a second, Jason and Chris.

But certainly the four models that were outlined today, none of them I think are particularly workable, and most importantly, I don't think any of them passes the test of being likely to materially advance the government's interest in reducing spam, and I just think that we should really avoid spending a lot of energy, unless we have a real confidence that there's actually going to be some effect on the other end.

When I spoke with the FTC officials at the spam conference in the spring, I think they were quite -- Brian Huseman and some of the folks there were quite aware of problems with this list, and I know Congress has entrusted upon you to consider it, but I would suggest the option be that the FTC say come back and say, "We've actually considered this, we looked at all the options, and we don't think it's an appropriate mechanism."

MR. CATLETT: I've been interrupted. I'll try to call back if I'm cut out.

MS. ROBBINS: Okay. Well, I think we're done with the Registry portion of this call, and now I would like to turn the call over to Michelle Chua. She's working on a study regarding the reward system, which is also known as the bounty system, and she would like to get your thoughts on that.

MR. SALSBURG: Before we do that, Colleen, Sheryl and I need to duck out to another meeting, but we want to thank you so much for taking the time to speak with us. This has been very enlightening.

CERTIFICATION OF REPORTER

MATTER NUMBER: P044405

CASE TITLE: INTERVIEWS IN CAN-SPAM REPORT TO CONGRESS

HEARING DATE: FEBRUARY 11, 2004

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

DATED: FEBRUARY 26, 2004

DEBRA L. MAHEUX

CERTIFICATION OF PROOFREADER

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

DIANE QUADE