EMAIL AUTHENTICATION SUMMIT

SPONSORED BY
THE FEDERAL TRADE COMMISSION
AND THE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

WEDNESDAY, NOVEMBER 10, 2004
8:30 a.m.

FEDERAL TRADE COMMISSION
601 NEW JERSEY AVENUE, N.W.
WASHINGTON, D.C.

P R O C E E D I N G S

- - - - -

MS. ROBBINS: Thank you all for arriving back for day two. We had a very exciting day yesterday and we expect nothing less from today. Before we begin, I just want to make a few housekeeping announcements. If you have a cell phone or other device that beeps, please make sure to turn it off. And panelists, if you could speak directly into your microphone, and if you want to respond to a question or comment, please just remember to raise your table tent.

Again we would like to thank the Direct Marketing Association and the Association For Interactive Marketing and Cisco Systems for providing us refreshments today.

Before we begin day two, I would like to introduce Commissioner Jon Leibowitz who will start off the day by giving us some introductory remarks. Commissioner Leibowitz is our newest Commissioner and started here in September of 2004. Prior to joining the FTC, Commissioner Leibowitz was the Vice President of Congressional Affairs for the Motion Picture Association of America, and held several positions on Capitol Hill, including Democratic Chief Counsel and Staff Director for the U.S. Senate Antitrust Subcommittee.

I am pleased this morning to introduce to you Jon Leibowitz.

(Applause.)

COMMISSIONER LEIBOWITZ: Thank you, Colleen, for making me look much more impressive than I know myself to be. Good morning. As noted, I am Jon Leibowitz. Thank you all for being here at this early hour, very early, to participate in the Email Authentication Summit. I want to open the second day by encouraging everyone in this room with an interest in authentication, whether an IP-based model, signature-based model, some other technology or some combination of technologies to work together to develop the tools necessary to help solve the spam problem. It's a goal we all share, and it's one that's attainable through your cooperation and creativity.

With that said, let me also thank the National Institute of Standards and Technology for cohosting this event, doing some of the heavy lifting yesterday in moderating the technical panels and helping us sort through the various authentication proposals and acronyms. From BATV, IIM and DomainKeys, to SIDF and CSV, not to be confused, if you live in the Washington area, with CVS.

Courtesy of my colleagues on the Commission, let me add the usual disclaimer: The views I express here today are my own and not necessarily those of the Federal Trade Commission or any other individual Commissioner or of my staff.

As many of you know, the Federal Trade Commission -- can you guys hear me in the back? Over there? Okay.

As many of you know, the Federal Trade Commission has a special interest in the electronic marketplace.   In the past decade, a whole new free-flowing exchange of goods and information has emerged, with huge benefits for consumers. As this cybermarket has blossomed, in fact even expanded exponentially, so, too, have technological challenges and the creativity of those engaging in cyberfraud and I suppose cybernuisance. Simply put, we can't let spam, spyware and spoofing, undermine the promise of the Internet.

Most people have a visceral reaction to spam, and it's no wonder why. Consider the statistics: Experts say that spam accounts for as much as 70 percent of all email and costs businesses $10 billion a year, much of that passed on to consumers. It also caused consumers countless hours of wasted time and immeasurable frustrations. Consider, also, that the vast majority of spam is deceptive, from false headers and phony identities to simply fraudulent offerings.

Just look at the spam in our inboxes, and here's some examples that came from one of my staffer's computers in the last week, ads for discount software, sometimes spelled W-E-A-R. Here's the tip: If they can't spell it, you shouldn't buy it. Unbelievably low interest rate mortgages, too unbelievable to be true, phishing expeditions by anglers looking to steal your financial account information and maybe even your identity, and ads for herbal Viagra and so-called vitality products that won't extend anything except the time you spend on your computer. That was a joke. I know it's early in the morning.

More seriously, spam is a problem that has literally hit home with me. I have two young girls, ages seven and nine, who have just started to navigate the Internet. The oldest one has her own email account, she's often online IMing her friends, and I am just extremely concerned and more than a little nervous that she and her younger sister are going to encounter this type of brazen and offensive spam and something far worse. Obviously we need a multifaceted approach to combat this serious problem.

Aggressive law enforcement is one part of the

Beyond law enforcement, though, we need consumer and business education to increase awareness and help users secure their computers and avoid being spammed and scammed.

The Commission is vigorously pursuing education initiatives and some corporations and consumer organizations are also beginning to help build consumer awareness. These efforts are crucial. But law enforcement and education alone can't do the trick. And rather than a do-not( )Tj0.0vigocaf rgBT36.00onyftuT1auhelps0.000

systems, we need to ensure balance and flexibility to accommodate various types of users.

To begin, any authentication system should protect the privacy, the anonymity and the free expression of noncommercial email. Political dissidents, victims of domestic abuse and others must be able to communicate freely and anonymously.

We don't want, in addition, to create unnecessary burdens or expenses for individuals and small business users. Any system has to be open, easy to use and backwards compatible.

Finally, we need to remember that spam is a global problem that requires a global solution. We don't need to give a veto to the French, of course, but we do need to be mindful of international -- it's early in the morning, so I understand that my humor doesn't go over really well.

We do need to be mindful of international standards and implications. In this vein, it was encouraging last month to see the Commission work with government agencies from around the world to develop a global action plan on spam enforcement.

Accommodating all these goals and interests won't be easy, but the benefits are important, so we need to move ahead, and quickly. This two-day summit is intended to foster a dialog among industry, government and consumers to explore various authentication approaches and hopefully to come to some sort of resolution. Although figuring out a workable authentication system isn't a panacea, it will help.

Authentication will help reduce phishing, spam artists will have a harder time hiding their identities and posing as legitimate businesses. It will help ISPs reduce their reliance on spam filters, it will help ISPs and law enforcement determine the domain where the spam comes from, improving our chances for identifying or identifying and catching deceptive spammers and deterring others. Most important, authentication will help ensure consumers' trust and confidence in the Internet, crucial elements in the long-term viability of e-commerce.

Last week, the Commission received a joint letter from dozens of technology companies. A clear indication that industry stakeholders are beginning to take steps to collaborate on authentication strategies. This summit is a terrific opportunity to share these ideas with more companies and constituencies.

So, let me conclude by turning to all of you, technology wizards, policy gurus, consumer advocates and Internet leaders, work up your plans and work out your differences. If we have competing authentication systems that don't work together, we may not have any that work. Let's not allow this to be just another spam discussion that rounds up the usual suspects, to paraphrase Claude Rains. Instead, this is a unique chance for the private sector to craft a market-based approach to ensure the continued success of the Internet. To be blunt, you don't want government to write the rules of the road here, you want to write them yourself.

So, finish your coffee, which I am going to do, go back to the summit and please continue to work together on behalf of all of America's consumers. I know you can do it and I thank you very much. Thanks.

(Applause.)

MR. SALSBURG: We're going to be starting the first panel of the morning, so if the panelists could come up and join me, that would be great.

Good morning. Can you hear me? Now can you hear me? Okay.

I'm Dan Salsburg, I'm an Assistant Director in the FTC's Division of Marketing Practices, and this morning for the next hour and a half we have eight people who have devoted a good part of their professional lives, at least recently, to fighting spam.

And we are going to ask them to take off their white hats and instead don the evil cap of a spammer, and come up with ways that they would go about defeating authentication standards. And these eight people are, beginning at -- where should we be beginning? Down here. Scott Chasin. Scott Chasin is the CTO of M Logic. Next to Scott is Tripp Cox, he is the CEO and Vice President of Technology for EarthLink. We have Brian Cunningham, who is not here, but maybe he will be somewhere coming soon. To my immediate right is Pavni Diwanji, Pavni is the Chairman and Founder of MailFrontier. On my left is Dr. Philip Hallam-Baker, who is a principal scientist from VeriSign. Next to Dr. Hallam-Baker is Keith Moore, from the University of Tennessee Knoxville's Innovative Computer Laboratory. Next to Keith is James Powers, who is the Vice President and General Counsel of ICS Network Systems, and President of the Data Rights & Privacy Advisors. And on my far left is Dr. Clay Shields, who is a computer science professor at Georgetown University.

Thank you all for coming. Let's begin with Pavni Diwanji. You're a spammer this morning, and you're spamming herbal Viagra, and let's assume that authentication systems have been put in place by the major ISPs, we'll just say, we won't identify which particular ones at this point, but how as a spammer would you go about, and let's say you're not a very technologically sophisticated spammer, how would you go about getting your spam through the authentication systems?

MS. DIWANJI: Well, that answer I have to say is very easy today. You don't even have to worry about exploiting technological flaws in authentication standards because all you have to do is have a zombie network or a zombie drone in order to then send out email on your behalf.

So, what we observe is, for example, for phishing attacks, about 30 percent of the email -- phishing email attacks generated is being delivered by zombies and they would still get through any kind of authentication standards that were talked about yesterday.

And on spam, I think that percentage is even higher. So, very easy to do.

MR. SALSBURG: Would you even have to deploy a zombie network?

MS. DIWANJI: Already deployed, right.

MR. SALSBURG: Well, would you even have to hire or contract with somebody who has a zombie network deployed, couldn't you just send your spam to those domains that aren't participating in the authentication system?

MS. DIWANJI: Yeah, absolutely. I was answering your question that if authentication standards were deployed worldwide, what would be an easy way to do it. I mean, today, if you think about, if you look around, I would say 45 percent of the phishing attacks and spam probably the same person doing the spam attacks are happening just from pure forgery. And you know there's a lot of authentication standards have antidotes to that, but it's kind of in varying degrees like the analogy idea is SPF is the aspirin of the world and Sender ID is probably a little bit stron 0.i I

MR. SALSBURG: Now, would any of the authentication standards have an impact on zombies?

MS. DIWANJI: I was actually pleasantly surprised to the introduction to CSV yesterday, so I don't claim to be an expert on it, but it seems like it's moving, it's at least trying to do something about it, which is a very pleasant thing that someone is actually thinking about the big problem, the big picture problem. But my worry is that we are all sitting here debating about different authentication standards and technological flaws and then there is this big part of the problem that's essentially social engineering, domains and zombie driven that is kind of being ignored today.

MR. SALSBURG: Do any of you have thoughts on zombies and how whether any of the authentication systems deal effectively with zombie networks?

MR. POWERS: I can offer. We are aware that Adelphia Networks is a large cable operator that is publishing SPF records, and the ability to use that information and take traffic that's emanating from that network has proven successful not against perfect zombies and well executed plans, but the records are able to be used. So, SPF is most the information being made available, can it be used, it be can used in some cases where you're analyzing the traffic coming from that network to detect whether you think it is a compromised PC. So it can be used.

MR. SALSBURG: Let's say these zombie networks are sending their spam through the ISP's MTA, rather than creating their own mail server, and sending out the mail via port 25, won't the spam appear to be authentic?

MR. POWERS: It will, and that's where a combination of things. The recognition that these are all arrows we're trying to add to a quiver and add these varying solutions, a combination of traffic monitoring coming from a certain network, you would then detect that that's an irregular volume of communication from an individual PC, that it looks like a stream emanating from that user, is inappropriate for the traffic patterns for that network generally. So, a combination of network sensing or observations combined with SPF near the scheme may be the way we need to work.

MR. SALSBURG: And this would be monitoring by the ISP where the traffic is coming from?

MR. POWERS: Actually, I'm the technical lightweight this morning, so please, I'm sure there are people who can talk about package shaping, IP monitoring and basic traffic analysis far more effectively than I.

UNIDENTIFIED SPEAKER: Louder, please.

MR. POWERS: Sorry. There are people who can speak about traffic -- analysis of traffic patterns, it's an essential element to look at the data flow coming from or across a network to detect what is in that data flow, and that's another form of network analysis.

MR. SALSBURG: Dr. Hallam-Baker?

DR. HALLAM-BAKER: I think it's a good thing to bear in mind that ISPs really do not want Trojans on their network, or zombies. That machine is eating up their bandwidth, and if they don't stamp on it, they're going to have a problem. And so, the authentication mechanism is not going to stop the zombies, but there's already a huge incentive to stop the zombies, because of the customer service complaints, eating up bandwidth and they're really unpleasant for the end users. And so, okay, they will send out spam, unless you've got email rate limiting in place. You'll probably see the ISPs looking for a Great Wall of China type solution. The Great Wall of China was not just built to stop the bad guys getting in, it was actually too long to be able to garrison it. You would have had to have the entire population of China garrisoning it the entire time it was built. The strategy was you allow the barbarians to get in, they attack a town, but by the time they're trying to get out of China with the loot, you've then got that section of the wall garrisoned, and you can stop them from getting out there and making a profit.

Maybe what we should be looking at is reverse firewalls so that if we could build into every cable modem or wireless router, build in a mechanism that says, okay, don't allow more than 200 outgoing ISP connections in a minute, or don't allow more than -- don't allow fake IP and packets, don't allow DOS attacks, then we could have the same sort of principle, deny the use of that host to the spammer or whatever other bad guy, make it useless to them. And maybe that's another way around it. But we're not going to solve it with this particular arrow, but we've got other arrows in the quiver.

MR. SALSBURG: Does this particular arrow of authentication have any point to it with regard to zombie networks?

DR. HALLAM-BAKER: Oh, absolutely. What we're trying to do here is we know that for every move that we make, the bad guys have got to countermove, at this point in the chess game. However, what we're doing is that we're moving our pieces onto the board into the more powerful positions, and we're limiting the scope of maneuver of the bad guys and we're not going to checkmate them with this particular move, but we're confining them to a smaller part of the board, we're taking their most powerful pieces off the board, you know, getting Sender ID out, that's equivalent to capturing a rook, and in chess, that's a very important move. If we can get Sender ID and the cryptographic mechanisms out, that's like we've captured the queen. It's not the end of the game, but it's a powerful mechanism.

MR. SALSBURG: And I guess the question is, while we're focusing on capturing the rook and the queen, those are coming through the front door, back on the side of the board are there a bunch of pawns about have to be sending out hundreds of thousands of emails an hour, to make it worth while. Because, you know, if you look at the response rates, they're tiny. You know, they're fractions of a fraction of a percent. And so if you've got to send out hundreds of thousands of emails, no home user has done anything like that. And if you can't spot that behavior as a network operator, or an ISP, well, maybe you should be cut off from the Net and put into the playpen and people should stop accepting emails from your customers, you know.

MR. SALSBURG: So, would you expect, then, that ISPs in the near future are going to be moving to rate limiting?

Scott, do you have an answer to that?

MR. CHASIN: About rate limiting? Yeah, absolutely, I think rate limiting is going to be a solution that ISPs embrace, however, I will say the sophistication of the Trojans themselves is going to be quite unpredictable where they go. Oh, I'm sorry. You know, think of the trickle attack: If you have 200,000 PCs under your control and you need to get 100,000 messages out an hour, okay. So, you send one, you know, an hour, for each zombie that you have under your control. So, the trickle attack is going to have some big impacts.

You know, it's interesting, I think, overall, if you look at the development of these zombie networks, and the Trojans that are associated with them, they continue to evolve with alarming efficiency, efficiency not only in propagation, but the community at which they're created. It's an underground, open source community whereby from the point of disclosure of a vulnerability, the exploit living in the wild, that time is compressing.

Even this week, with I believe it's My DMAI [phonetic], which was announced on bug track October 24th. We saw a new worm that took advantage of that.

So, the time for exploitation within a payload is compressing. That said, I think that we have some serious concerns as to the motivational elements behind the creation of these tools. It's not egocentric hackers anymore, it's, you know, economically motivated criminal elements in an organized fashion that are deploying these technologies. And so, I think that's a real concern from the perspective that the machines that they're exploiting have vulnerabilities, but the infrastructure as a whole is extremely vulnerable.

So, from that perspective, I can draw some -- I can give you some ironies here, some ironic notes. We're trying to talk about Sender ID and SPF as an authentication mechanism that is going to be based on DNS, which has no authentication itself. DNS has no authentication. In fact, what's ironic is that DNSSEC, which was announced in '95, is just now making it through final RFC status. So, which means that there's no deployment for it. DNSSEC, you know, basically provides the signing of DNS packets, which by the way, DNS spoofing, cache poisoning, these are realities. And I believe that the shifty nature of those that are employing these technologies will start to look at these different threat factors, because we're changing the paths. We're changing the easy paths.

So --

MR. SALSBURG: Well, Scott, one thing you implementing efficacy authentication and implementing port blocking so that their email users are not taking advantage of compromised hosts out there on the network and other places. And I think you will continue to see ISPs take aggressive measures to make sure that criminals are not using their services to defraud consumers.

MR. SALSBURG: Well, one of the things that we've noticed at the FTC is that in recent weeks, a major ISP has announced that it's offering free antivirus software to all of its members. Is this a thing that all ISPs should be doing to prevent the spread of zombie networks?

MR. COX: I think so. You know, for better or worse, ISPs have been left to the responsibility of caring for consumers' personal computers, and that's a huge cost and burden to us, but it's where we find ourselves. So, it's almost worth the cost of providing them antivirus support so that we do not have zombies, massive networks of zombies under our domain.

MR. SALSBURG: Keith Moore? Scott Chasin mentioned the fact that SPF and the path-based approaches here are based on the DNS system, which itself is not authenticated, and he talked about something called DNS spoofing. Could you explain what

DNS spoofing is and how a spammer would go about doing that?

MR. MOORE: Well, basically DNS is insecure, so if you make a query, then essentially you don't know where the response is coming from, you have no reliable way to know. So, if an attacker can anticipate when a DNS query can be made and provide an appropriate looping response at about the right time, then he can fool the party pursuing the DNS query into thinking it has gotten a valid answer. So, until you get the DNS deployed, it would be inappropriate to comment about that.

And he also mentioned cache poisoning which is a similar technique where it's basically a DNS cache gets an answer from someone it believes -- whether it's -- usually it's an additional information field of the response. Then any party that uses the same cache to make a future query will get that answer, even though it didn't come from an authoritative source.

AUDIENCE MEMBER: (Inaudible).

MR. MOORE: Basically, right, it's a low probability -- well, like I 0.inappea Bas7rthdayw

212 attac6tr?4 412.8000mr(7h .0W .0W .0W .0WT1.0000aFct2rr0 1.E7kt A2rr0mdw

what that exchange was about, if somebody could translate it?

MR. MOORE: There's a request ID and the request and the response has to match that request ID. It's not anything that's cryptographically secure, it's just that it's basically designed to match queries and responses. So, you have to either get that or provide enough responses that you're likely for one to match the query.

MR. SALSBURG: So, depending on the number of requests you send out, if you send out enough, you're going to get back the right response?

MR. CHASIN: If you send enough responses, you or last week, new worms that have come out, which if you're looking at it from a phishing perspective, these new worms simply modify the hosts file on the affected machine, which means that, you know, once the machine is infected, essentially the facilitator of that worm can basically intercept the web session regardless of a carefully crafted phishing message.

So, what that means is, without the end user knowing what's going on, because they didn't actually follow a link in an email message that was a call to action to a phishing site, they simply went to their bank's website in a normal process, without, again, a direct call to action by the spammer, or by the criminal facilitator.

So, those are, I think, examples of early signs to look for in the exploitation of DNS.

MR. SALSBURG: Before we move off this subject with DNS, let me just see if I understand it. If I'm a spammer and I either spoof the DNS for Amazon.com or I've poisoned its cache, I can at least temporarily redirect email traffic that's going to Amazon to me?

MR. MOORE: Yeah, if you do the right thing. If you poison the cache that was inputted in, you can do that. So, it's a separate attack from just making someone believe that your message is legitimate and you can actually redirect mail, you can redirect, you know, web traffic, all those things, all those vulnerabilities exist.

MR. SALSBURG: So, the risk here is that there are vulnerabilities beyond masquerading someone who is using spam.

MR. MOORE: Essentially every location on the Internet uses DNS, and so every application is vulnerable to this.

MR. SALSBURG: Brian Cunningham, your tent wasn't up, but I thought you wanted to comment.

MR. CUNNINGHAM: Yeah, that's great. One point I guess on what Scott was saying, there was a recent attack against a large bank in the southeastern region in Atlanta, about three months ago, and sure enough they had honey pot accounts, everything, they had a phishing attack reported to them, the attackers actually used DNS spoofing and cache poisoning against the bank itself, so when the bank went to the site and went to try to find the servers, all of the servers looked like they were down, and each hop along the way they actually had more cache poisoning put in place so that the bank never even saw that there was even a problem.

So, it's more than just the end users, it's the people actually trying to put out the fires that are actually being directed towards this DNS cache issues.

MR. CHASIN: I'll just add that for those that have, you know, those financial institutions represented here that have a concern and interest in phishing and others that have legitimate, you know, concerns obviously, you know, finding large caches, DNS caches, there's another attack, which is, you know, basically cache snooping, which means that anybody can go through and query large DNS caches to find out if the pool of users behind those DNS servers are communicating, let's say, with Citibank, Wells Fargo, Visa.

So, not only is there the ability to exploit these weaknesses, yes, it requires sophistication, but you can find, relatively easily, pools of users that are most likely to visit those sites.

MR. SALSBURG: Pavni Diwanji?

MS. DIWANJI: Thanks. One comment, and I don't want us to lose sight here, I think it's not even necessary for the criminals to go this far. I just want achieved. I just wanted to make that point.

MR. SALSBURG: That's a great point. And I think we all agree with Pavni Diwanji that from the standpoint of spam, if we get concerned about DNS spoofing and cache poisoning, there are far more serious consequences for the Internet than spam, and so maybe there should be some other group that's really worrying about this than our group up here.

DR. HALLAM-BAKER: Well, if it's broken, then we should go fix it. The DNS is not cryptographically secure, but it isn't entirely insecure. In practice, there's a reasonable level of security in there, if the have the policy encumbrances, the interactions between everybody, between the users. It's something that can be settled with a much smaller group, much smaller number of people who have to make changes to get the infrastructure to be secure.

And it may be cryptographic solutions that we need, or it may be just a small tweak, a small improvement that's more easily deployed that doesn't require large resources.

MR. CUNNINGHAM: Can I just add one point? I mean, I know that we're diverting away from DNS, but DNS drives everything. And I think it's immensely important that we recognize that because if we adopt solutions that are heavily dependent upon DNS, we're really developing a whack-a-mole problem, because what's going to happen is necessity is the mother of invention. As soon as we take the focus off of the SMTP protocol and put it onto DNS, I think we're in for really a world of hurt, to be honest. Because --

MR. CHASIN: And I'll just add for those that want more information about these threats, they're well documented in RFC 3833, and so I would review that for a good overview of these types of DNS attacks, and how they may be exploited.

MR. SALSBURG: Let's shift gears back to the unsophisticated spammer, the one that's not going to go out and poison the cache. Isn't the most likely thing a spammer is going to do after authentication is widely deployed is have a whole series of domains that are authenticated and once one gets cut off by an ISP, use the next one?

MR. CUNNINGHAM: Well, that's the situation that we're in right now. I'm sorry, go ahead, Pavni.

MS. DIWANJI: I think they already do. Like our SMM is about today if you look at spam, what's interesting is if you look at the recent outbreak of the 30 percent of the domains that are already authenticated, so what you can see here is basically that it's the fastest and upcoming community of authentication standards is the spammers.

So --

MR. SALSBURG: So does that mean, Tripp, are you at EarthLink filtering anybody that has an SPF record?

MR. COX: No, we're not filtering on SPF yet, we're still evaluating SPF along with several other authentication standards.

MR. SALSBURG: But that's not something that's directed just at spam, the fact that it has an SPF record?

MR. COX: No, I wouldn't say it's an indication of spam, necessarily. Obviously spammers do want to do whatever they can to get their messages through and they will adopt and embrace whatever sender authentication protocols we put out there. What we really have to do to get to the root of the problem is to make it uneconomical for them to do that or legally risky enough where they're not willing to take the risk.

MR. SALSBURG: Spam is based on margins. Because it's such a low cost, does increasing the cost slightly naturally have an impact? Does requiring someone to have multiple domains and spending $6 or $7 every time they have to get some more messages through impose enough of an additional cost to actually have an effect?

MR. COX: I don't think so. I think there are a number of things you can do to get around that, one of which is to register a domain and then create a dynamic tertiary domain w v'   every time they have to get some more mess going to look for a place that is insecure and open and the global nature of the Net and an example of this happened just last week. The Spanish Data Commission was here in Washington speaking about data protection and privacy issues which phishing is now having heavy implications for, and noted that Germany, today, does not have a designated federal official in the German government that is tasked to handle the spam problem. They're working on it, but when the meat clever Trojan which hit last week, it was directing all of its traffic back to query, about 60 domain names, and where were they? Russia, which we all expect, the renegades within that. But Germany as well.

So, if today's unsophisticated spammer can go to a first rate developing nation or a nation like Germany, what does it say about every other node on the Internet? And I think the unsophisticated spammer knows there's a world of opportunities and the fractured nature of our response is something that I kind of offer the panel.

There's an analogy, perhaps, that in the early nineties and late eighties, the credit card community started noting fraud occurring with credit cards on the electronic commerce network, the backbone that clears all the electronic transactions. They started analyzing that traffic. That was just one of their solutions including putting cryptography on cards for identification, part of that panoply of solutions.

So, I hope that maybe the diverging nature of the discussion reflects that absolutely nobody gets a panacea solution, but the unsophisticated spammer realizes we're a fractured community, and that's the one thing we can do, share more information amongst ourselves. So that you know there's a lot of pockets of solutions, but are we sharing enough information about what we encounter so that we can collectively respond?

MR. CHASIN: I would note that our confusion on these topics are -- it's their opportunity. You know, that said, if you -- I kind of was asked to do this as far as put the black hat on. I broke it down into infrastructure and security, I think we've covered that with DNS. Self publishing, you know, there's something like 10,000 plus domains registered every day, 41 million domains on the Internet. There's something like anywhere from 13 to 20 million mail exchange hosts. Those numbers, yeah, I'm just kind of, you know, high level here.

Self publishing I think is going to continue to exist. The display, the pretty name display capabilities, lack of configurability on the client side I think is going to add to more of that confusion.

The other area is that they could simply ignore it. Ignore SPF, Sender ID, excuse me, all together, and enjoy a few more years of freedom, most likely. And so when we talk about the unsophisticated spammer, I think we noted earlier that the majority of spam today comes from zombie networks. And so I would say that that's a sophisticated facilitator that has the ability to deploy those networks.

MR. SALSBURG: Dr. Hallam-Baker?

DR. HALLAM-BAKER: I think that when you're looking at the domain problem, the registering the domain problem, the first thing that you've got to observe is that the majority of spam is just criminal. I mean, after CAN-SPAM was passed, it changed from being quasi legitimate to, "okay, we're not going to make any pretenses out, you know, now we're going to do the phishing attacks, we're organized crime, we're the Mafia."

And so if they've used a legitimate credit card, then one solution is, as a lawyer, you can go and sue them. Go -- we've got somebody, they're interested in doing something criminal, put the police onto them.

So, of course, the bad guys are not going to be using legitimate credit cards. And so now we have the issue, okay, a domain name is being bought on an

talking with the financial services industry, the financial services industry, yes, everyone is going to adopt whatever is available, but what they're primarily looking for is an end-to-end solution, and basically a server site authentication, reputation server. What this allows them to do is actually see what's happening with their outbound mail and see what's happening with people actually trying to phish against them. That allows them to have realtime reports, realtime alerts and actually a system that can evolve into message tracking and everything.

And so, I just want to throw that out there, because I think that whenever we build the necessity for basically organized crime, any phishers out there to basically take a new perspective to get around authentication schemes, I think that what's going to happen is we're going to start looking toward end-to-end solutions.

MR. SALSBURG: Both you, Brian, and Scott have drawn a distinction here between phishing, spam and the effects of authentication. To sum it up, would an example be with an authentication scheme in place, I could have confidence that the message that claims to be from Citibank.com actually came from Citibank.com, but the problem is if it's from Citibank-billing.com, a consumer may still think it's from Citibank.

MR. CUNNINGHAM: You have two, you have two problems, yes. You have the Darwin effect, I mean, that's huge right now. I think there's still about a third, about 33 percent of all users will basically respond to those emails, even if it says I want to steal your money.com but I'm acting like Citibank, 33 percent of people will still click on it. It's amazing right now.

But I think primarily the important point is it's just like RMX. RMX was a great authentication standard in '96 and '97,.0000bFgPTdcdsv0 0cting like Citibank,aran of course they're trained through history to basically trust it. So, to call it -- I mean, I was just saying like to call it Darwin effect is probably not accurate, I think everything is of our own doing.

MR. SALSBURG: I apologize.

MR. COX: If I could paraphrase, Brian, I think what he's trying to say is continuing education of both businesses and consumers is critically important as well.

MS. DIWANJI: That's a fair statement.

MR. CHASIN: I would also suggest that outside of, for again, those institutions who are the victims here, outside of the consumers. You know, outside of embracing the authentication technologies, two-factor authentication can help as well. Not necessarily for man-in-the-middle attacks, but the ATM card is a good example of a device that we all carry, yet when you log onto that banking site, it's usually a user name and password.

So, I congratulate AOL in their efforts for pushing a two-factor authentication device. I think we should see more of that from the financial institutions as well to help minimize and mitigate risk.

MR. SALSBURG: Can you give us a 30-second description of how two-factor authentication works?

MR. CHASIN: Your ATM card is a good example. To some degree it's a physical card that you carry, as well as a secret that you have. So, you have to have the card as well as the PIN number in order to access your account.

MR. SALSBURG: And this differs from the typical user name and password, which the only secret is the password.

MR. CHASIN: In the Internet world, it's usually a device which generates a number that corresponds to a seed that is embraced by the service provider.

AUDIENCE MEMBER: What you have versus what you know.

MR. CHASIN: Exactly.

MR. SALSBURG: I think I've been handed a two-factor.

DR. HALLAM-BAKER: Unfortunately that's an engineering example.

MR. SALSBURG: But it does say VeriSign. I'm sorry, I have to decline because of the ethics rules.

DR. HALLAM-BAKER: It costs way, way less than $25, so you're allowed.

MR. SALSBURG: Where can I buy this?

DR. HALLAM-BAKER: Actually, this was an open standard that we've been trying to create to make it nonproprietary and to get back to the hardware part. Because what I would like to see is to get rid of the tokens and have that capability built into, you know, every mobile phone, every RIM pager, make these dirt cheap. Make them so that they're $2 bucks. Make them so that we can give them to school kids so they can identify themselves in online chat rooms to protect themselves against pedophiles.

MR. SALSBURG: And how would you apply a two-factor authentication device with the sending of email? When I get onto my email, I have to do what?

DR. HALLAM-BAKER: Oh, I don't think you do it for the sending of email, it would be for when I go to my online bank and I log in and I press the button, it gives me a number, I type the number into the bank site, and then that is a one-time use password. In Europe, they give you little cardboard strips where you scratch off the next number in the sequence and that's your password. And so you can do this with a really low tech or really high tech.

MR. SALSBURG: So the idea here is that the domain level identification can keep you from the phishing attacks that claim to be Citibank.com, but you're going to need something more?

DR. HALLAM-BAKER: Right.

MR. MOORE: People have made the statement to the effect that email authentication, domain level authentication would decrease phishing by making it difficult or more difficult to impersonate, say, Citibank. And I don't want to pick on them in particular, but I wonder to what extent as long as people are running lots of insecure hosts or hosts that are running vulnerable operating systems, which is by far the norm, you know, this is what makes these zombie nets possible. The number of attacks that you can do with those kinds of platforms is considerable, you can steal host keys, you can attack DNS from there and poison caches. You can, you know, you can use those to say I want to spoof example.com, while I'm going to compromise some of their hosts and then I can send mail from their hosts. And again, there are so many things that you can do if you break into computers and it's still very easy to do.

So, as long as we're looking at authentication as one thing and two-factor authentication helps, but only if it uses something in the sender's head, if it's using a piece of hardware that's attached to a machine, it still can be compromised.

things that are actually general security risks but seem to be moving away from the discussion of spam and the authentication of spam. And a lot of what we're talking about is actually technically feasible, but people who are going to be attackers and send spam are not going to go to the lengths and expense if they possibly can avoid it. We talked about undercutting their margins.

So, they're really going to do what's the cheapest, simplest and most straight forward thing they can do. And I think we've touched on a lot of those. I think for a long time while the system is in transition, they're just not going to authenticate if they don't have to, and can avoid doing that, because even if their rate of success may go down, it's still going to get some through. And as long as they have 0.001 percent instead of 0.01 percent, they're still going to be successful.

After that we're looking at what can they do to be authenticated, and we talked about being able to authenticate themselves by setting up their own domains and we've talked about being able to get other people to authenticate for them. There's also, which this came up, I think, the possibility where spammers will be able to get keys, either cracking them or stealing them, and being able to forge messages themselves for a while.

So, I think that all of the things we've talked about, the security aspects do play a factor, but really they're not going to come into effect for a while, because now it's just so easy to not have to do that stuff.

MR. SALSBURG: Once the major ISPs are using the authentication system, if the spammers were to target those other ISPs and other operators and mail servers, wouldn't they come into compliance with the authentication standards pretty quickly? You know, if I'm an operator of a mail server and suddenly all of the spam in the world is being directed at me instead of AOL, isn't my reaction going to be to immediately publish --

MR. SHIELDS: Well, if it's being directed at you instead of at AOL, and you're not checking authentication. The problem is that authentication just tells you for sure if somebody sent something. It's possible that if the authentication fails, the person who claims that they still sent it, it's just that it's not proven, right?

And so, if I understand your question correctly, it really affects more people who are receiving the email to authenticate it rather than the people who are sending.

MR. POWERS: If I can offer, I think there's a reliance on spammers to recognize that were the ISPs authenticating and doing the right thing, I want to catch the end-to-end solution. I think the end-to-end solution is the reason that the Commission particularly wants them because they recognize the behavior out on the Internet is so disparate and so different. Therefore an end-to-end solution offers the illusion that if I stay within the system, it's a secure transmission.

But I think the point is would you have renegade networks, you have secure ISPs offering all the authentication, and then just like the telecommunication network, if I have insecure phone calls coming in to my Verizon network or my SBC network, when do I cut off those calls from Romania because I know they're all using stolen Visa credit cards.

Those are the practical matters that spammers absolutely recognize, but to refuse traffic en masse and to block out the renegades that aren't complying is a very bold gesture. And right now, a lot of people won't refuse traffic from Hotmail, MSN, AOL, and that's one of the reasons that the IOS tools that my clients use is focusing on those networks because people are loath to cut off traffic from them. So, you have a very

taking care of everything and being a silver bullet, I really think that that is incomplete. I think what's [illegible] have to bear in mind, what happens when something goes understanding reputation and it would probably be an easy -- I shouldn't say that -- should probably be something to look at as far as other inputs into reputation very early on.

MR. SALSBURG: Dr. Hallam-Baker?

DR. HALLAM-BAKER: Yeah, there seems to be a bit too much agreement, so it's time to disagree. I don't understand what people are mentioning by this end-to-end model. It seems like it's not an end-to-end model at all, it's an edge model, and I always thought the end-to-end model was bogus.

As far as Keith mentioned earlier --

MR. SALSBURG: Maybe you can tell us what is an end-to-end model versus an edge model? What's the difference?

DR. HALLAM-BAKER: Well, the original idea of end-to-end was that it was an argument about complexity and where you put it in the Internet. And the idea was that you put the complexity at the end of the communication, so from my pager through to the other end ultimate recipient, and this kind of like got turned into a dogma where it kind of like got compliant to security, and the basic idea was that if I encrypt it from the pager all the way through to the recipient, then, you know1hFBTua,G: Ma3n.0000 0.0000 cm0.00 0.00 0.00 rgBT36 tapping in the middle can't do that.

And so this whole thing got us into a huge amount of political entanglement. If you look at the successful security models we have on the Internet, they're mostly edge models, and what we do is we secure from the user to the edge, from the edge of the Internet of their ISP to the ISP that they're talking to, and then from that ISP on.

I mean, the end-to-end model has led to all sorts of silliness, like people are saying, "oh, get rid of your firewalls," they're not according to the end-to-end model.

But what I really wanted to comment on was the other ideology, which I have heard coming in here, which is that bad security is worse than no security, because people get a false sense of security. You know what? The end users who we're talking about, you know, the typical victim of one of these 419 scams is a 70-year-old grandmother, possibly with Alzheimer's. These people have a false sense of security. Just from the fact that you give them a manufactured object that appears to function.

So, giving them more security is not going to lead them to a false sense of security. They've already got that false sense of security. And then just to finally disagree, Keith said that the majority of the people are using insecure operating systems. That's untrue. Everybody, every single person is using an insecure operating system. There isn't an operating system out there that has been designed for real end user security. Most of the security models that we're applying were designed in the 1920s to secure military secrets on shared computers, where you had multiple people sharing the same operating system.

And what we've got to do here is to move into a world where we're providing security for real people and not security for geeks. You know, we spent the past ten years amusing ourselves, and, you know, not noticing the fact that, you know, the Mafia is out there and they're out to make money.

MR. SALSBURG: Speaking of security, one of the reported benefits of the crypto-based authentication models has been that it provides better security over the path-based models. Is there truth to that?

MR. MOORE: I think that's an over-generalization. There are attacks that are more easily foiled with, you know, the properties of your domain and the properties of the IP address that you come from and there are attacks that are more easily foiled if you have, you know, keys that reside on a host that people have to sign. So, I think if people say one is better than the other, you have different ways of compromising each.

Now, once you get something to a separate hardware device that you have to plug in in order to send mail and then you also have to couple with something you know, you get two-factor authentication that's pushed to the level of something that is not easily remotely compromised, because it's not full-time attached to the network. You know, then, in order to compromise that, then I have to get into Phil's brain and, you know, do the Vulcan mind program on him and say, reveal your password and then I have to steal his device. Okay, that's hard. But as long as we're having to compromise things that are not well constructed and attached to the network, and whether that's DNS servers or whether that's individual hosts or whatever, those attacks are still feasible.

MR. SALSBURG: Clay Shields?

MR. SHIELDS: I would just like to mention we talked about two-factor authentication, and it is much, much better. There's no doubt about it. But I shudder to think that my mom would actually have to have a hardware device, because she would probably misplace it -- no offense, mom, if you're listening. She would probably misplace it, she would lose it, leave it at home and be unhappy about it. And if you look at the organizations that have to support a large number of customers, like the large ISPs. I know the one that is doing that is charging additional for it and not requiring it of everybody and I can't imagine what their costs would be if they had to issue it to everybody to maintain control of these things and just the overhead of managing the cost to the users with them. So, I don't see that coming into the global effect any time soon outside of the small audience.

MR. CHASIN: You have to look at the cost and the risk benefits here. You have to look at, you know, the success rate of, you know, this person finding their car keys. You know, their ATM card. So, I mean, it's end user education and it's awareness, and it's the cost factor. I mean, you know, the end result of all these phishing attacks means, you know, millions if not billions eventually lost, is that enough of a catalyst to start issuing these tokens?

MR. SHIELDS: Well, it depends on who pays the cost. Right now the cost of losses of fraud is spread across all consumers. I'm sure if Visa or MasterCard had to pay those costs, and couldn't pass them on to their customers, then it would be different.

MR. CHASIN: It's something to explore. I mean, we all hope for -- you know, or some of us -- the day that you have the biometric send button on your mail client. But, you know, we're way off from that.

MR. SALSBURG: We probably are way off from that, but with zombies residing on computers, how would a two-party authentication -- a two-factor authentication actually work?

MR. SHIELDS: Well, I think the assumption here is that we're doing some sort of authentication of the individual sender as they send mail, and so if we were going to use some sort of authentication -- I'm making this up by the way, because I don't know of anything that can do that, but if you're going to do that, it would be -- you would have to authenticate not only some password, perhaps not only a password that you know, but something that's generated by your device to your outgoing mail agent so it would send mail on your behalf.

MR. SALSBURG: Would you would have to do it for each particular mail message?

MR. SHIELDS: Yes, essentially, because the way most of these things work is they're short-time, nonreusable passwords.

MS. DIWANJI: We actually have seen the phishing attack that repeats one flavor of this two-factor authentication already just to give people -- I'm saying that we're already seeing a phishing attack that is trying to defeat this two-factor authentication, one flavor of the two-factor authentication. So, all of these schemes I think are defeatable, right.

It's going back to Scott's point, which is it's a cost benefit thing. Now you're putting the burden really on the other party and we are at one thing eventually. That's what we are talking about.

MR. CUNNINGHAM: For me, I mean, whenever we're talking about this two-part authentication, I mean, when we're talking about these disposable passwords and all mean, I just want to make sure that people understand what we mean by end-to-end solutions. I'm not talking about cryptographic approaches, end-to-end and unpacking data. I'm talking about the mere fact that I'm sending from an email server, I know what I've sent. That email server has log files of everything that it has sent. There are technically ways that you could simply query back and say did you send me this email, yes or no.

And so we're not talking about any type of unpacking of data, any type of encryption scene, we're just simply talking about hey, I got an email from you, did you send it? And with computers, we can automate that entire process.

MR. CHASIN: I would just add real quick that, you know, phishing, the call to action of phishing today is email. That's not necessarily true tomorrow. Again, it could be the modification of the operating system hosts file, which has a web redirect and a browser. So, the call to action is going to evolve, that's for sure. So, that's why I'm focusing on two-factor authentication at the destination site, to mitigate the risk even more.

Of course, there are challenges, the man-in-the-middle attacks and others that are out there, but it is about raising the bar, the continued movement of building our defenses, because the other side has sophistication and motivation to continue to build up theirs. So --

MR. SALSBURG: Brian Cunningham, you've analyzed both DomainKeys and IIM from the standpoint of how the cryptographic algorithms work.

MR. CUNNINGHAM: Um-hmm.

MR. SALSBURG: Are there insecurities of either how those algorithms work or the way that the keys are posted?

MR. CUNNINGHAM: Well, the issue for me is really the security of that salt value or that seed value. I mean, who in this room remembers in '92 when MD4 was considered unhackable, then MD5 in the mid-nineties, and then SHA0, and now there's rumors that SHA1 is hacked. I mean, for us to come in and actually say that encryption will take care of everything, there's no possible way. Grant it, I think it's a wonderful solution, I really do, but I think it's naive to say that it's going to solve everything.

For me, it's really about the integrity of the salt value. For example, AOL, there was a gentleman recently that sold 93 million email addresses for AOL. He's been prosecuted. Now you have organized crime involved and you have salt values out there, seed values, everything for your keys, they're going to become prime targets for attack.

I think it's a necessary method, I think that it's a valued method, but I don't think it's going to be the silver bullet.

MR. SALSBURG: One of the questions about the cryptographic approach that I have is there's a lot of talk about the amount of computing power that would be needed to crack the hacks, and how difficult that is. And you just raised the issue of how every time there's some sort of encryption standard, soon, after a number of years, it gets hacked. With the deployment of zombie nets, could that power of the zombie nets be used to --

MR. CUNNINGHAM: Oh, yeah, completely. That's how they're cracking SHA1 right now, or rumored to be cracking it, using raw computing power and putting a zombie on there and distributing computing. But more importantly, I mean, I think Phil would be more appropriate to talk about this, but it's my understanding that the number one rule to cryptography is the fact that you need to -- people do not need to know or they should not know what the actual data is that's being encrypted. So, if we start using encryption screens that are basically open source that we're saying, all right, we're going to take the "to address," the "from address" and the time stamp and we're going to encrypt that and put a signature here, now I know what you're actually encrypting. Now I have a road map from actually trying to hack your network.

And so I don't know if that's possible. I think it's possible, but it does make me a little uneasy whenever we actually have a road map for what our cryptography system is actually using. I think that's a concern.

MR. COX: Just to respond, I think whether it's digital signatures or two-factor authentication or calling back to the SMTP host to ask whether or not it actually did send the message, we could play the what-if game all day long, and in fact until the cows come home, and I think what we're not really discussing is picking the low-hanging fruit and doing the things that are easiest to implement and have the biggest benefit.

Yes, DNS could be compromised, yes keys can be compromised, yes, two-factor authentication could be compromised, but the likelihood of that is very low and the benefits of those technologies are very high. And I think that that's something that we need to keep in mind as we talk about what is beneficial for us to do at the moment.

MR. SALSBURG: Dr. Hallam-Baker, Tripp raises the point that authentication schemes probably don't have to be perfect to be useful. Is that something you agree with?

DR. HALLAM-BAKER: Absolutely. And since this is cohosted by NIST and SHA1 is a Niststandard, I think that somebody should come in and protect it and defend them. The algorithm that was broken was SHA0. SHA0 was the first version of SHA, and just -- it was published as a federal standard, and a few months later, there was a revision made to it.

When the first attack started to be published on MD5, MD4 and MD5 were both developed by Ron Rivest at MIT. SHA1 is also a development of MD4. There are similarities in their approach and when we analyzed how MD5 was being attacked, the defense that are being put into SHA1 by an unnamed federal agency turned out to protect against that particular attack, it's the expansion function in SHA1, so now we know why it's there.

The practical upshot of it is that SHA0 has been broken, but nobody has broken more than 40 of the 80 rounds of SHA1. So, nobody is breaking SHA1 using publicly known cryptographic techniques. I very much doubt that the organized -- that organized crime has access to better cryptographic analysis than is available in the public sector.

Now, governments may. You know, there may be world governments who can break SHA1; however, even if the bad guys could break SHA1, all they would do, in the usage that we have with IIM and DomainKeys, they would only be able to forge a message, at worst.

And so, even if SHA1 was broken, it wouldn't be catastrophic breakage of the whole system, because nobody is going to dedicate a botnet for six months to cracking a SHA1 message to send out one spam. The risk and reward isn't enough. And so what this comes down to is it's the margin for the attacker. Is the cost of breaking the system less than the reward?

MR. SALSBURG: Clay Shields, if I were running a botnet and one of these crypto approaches were in place, instead of using the botnet to try to crack the hash, couldn't I just set the bots in different random keys?

MR. SHIELDS: So, let me just mention a couple of things about crypto really fast. First of all, crypto isn't dead, despite all the news. If you actually look at what's going on with the hash functions, the attacks that have been discovered are actually not particularly practical attacks. Because they're -- the community is aware of these attacks. Now I can guarantee you that new algorithms are going to be developed in the near future which will be more resistive to them. So, as these attacks come out, the algorithm cells are going to get better. So, crypto is not a solution, it's just a useful tool.

When we talk about crypto, we can talk about encrypting, we can talk about hashing the -- a hash simply takes a large document, perhaps, or a computer file and it provides what is essentially a unique fingerprint for that file. When I say essentially unique, the chances of collision, are, you know, two to the 160th, which is infinitesimally small that two documents will generate the same hash.

Encryption takes a document and renders it unintelligible. It takes the information and translates it into something that isn't immediately obvious. So, hashing doesn't hide information, it just verifies the integrity, where encryption essentially hides the information.

So, the question is if you had a botnet, would it be more useful to crack keys than send messages out? It might be if the bots that you had were not located where you wanted them to be. For example, say I wanted to be able to send email, and again I apologize for picking on Citibank, but say I wanted to send out email to Citibank and I did not have a machine in their domain to send email out. It might be better for me to set the machines to try to recover the keys that I could use to encrypt or hash things and send them out, rather than sending the mail directly.

Does that answer your question?

MR. SALSBURG: Sure. One of the domain level authentication proposals that was discussed yesterday was BATV, and Doug Otis described how it could be used in a way that involved private keys instead of public keys. Does that provide any -- is there a different analysis in terms of the cryptography?

MR. SHIELDS: When we talk about cryptographic algorithms, there's essentially two common types, there's a public key cryptography and a public key or a shared key cryptography. In public key cryptography, I generate two keys, one of which I keep to myself and it's called my private key, the other one I can disseminate to everybody in the room and it's my public key. Anybody can take something with my public key and encrypt it. Once they've done that, I'm the only person who can decrypt it.

Conversely, I can take my public key and I can encrypt something with it and send it out, and since everybody has my private key -- excuse me, my public key, they can decrypt it. Now, in that sense, what that's proving is I'm the person who encrypted it, because only I have the appropriate key.

In a shared key crypto system, we have something that's agreed upon, there are methods to do this on the fly, but typically we agree upon something in advance. And we have this shared secret that we use as a key.

The public key crypto systems are not known to be invulnerable. They're all based on hard mathematical functions that are believed to be easy to do one way and difficult to do the other way. As techniques in math advance, it might prove that the things we thought were hard, actually there might be a new solution which makes them easy.

So, in public key crypto systems, they are based on things that we believe to be hard, but were not. We don't know for sure. The shared key crypto systems, the ones that are in use, we believe that the best way to attack those is by brute force certs through all the key space. The public key crypto systems, the key sizes tend to be about an order of magnitude larger for roughly the same time, using the techniques we know now in shared keys. Sort of my crypto primer for the day.

MR. SALSBURG: Brian Cunningham, when you talked earlier, you talked about the issue of cryptography and the 40-bit encryption standard used by most European governments. Can you describe what the issue is there?

MR. CUNNINGHAM: Well, for me, it's one of a question. If we are going to adopt, you know, I think we should adopt a level of cryptography, but if we are, are we going to be hit with basically federal sanctions that we can only use 40-bit encryption on anything that has the possibility of going outside this country, because right now there's current legislation that you can't do that.

MR. BURR: No, no, no. I'm sorry. That's just not true. I'm Bill Burr from Nist. That's really just not true. There's -- there's about five countries that you have a problem exporting strong encryption to. I mean, the Bureau of Export Affairs, they changed their the middle of the Clinton administration when we were trying to control cryptographic experts, or cryptographic exports. There's a lot of stuff out there that does it. It's actually done by taking reasonably good cryptography and then publishing part of the key so that somebody listening gets a good part of the key for free, but 40-bit cryptography, except as a legacy, is a dead issue.

MR. CUNNINGHAM: Okay, question answered. So, we can export any level of cryptography across?

MR. BURR: As a practical matter, if it's not in a weapons system, you can export 128-bit, 256-bit, AES. Cryptography is as strong as we know how to make it. And there's never actually been in U.S. law a provision to stop you from using it, just from exporting the software or the hardware that would implement it.

MR. CUNNINGHAM: Right, well that was basically the question, because if we implement this in the

system whether it is cryptograph or IP, you know, it's going to try and stop forgery and that really only makes up for about 40 percent of the problem today, as we see it today.

The bulk of the issues around social engineering attacks as we talked, and zombies, and so I would say that given the near term, we do have to think about those two issues, and longer term, definitely, because that part is continuing to grow.

MR. SALSBURG: Why don't we open it up to questions. How about the gentleman right here in the front?

MR. ELBEY: Matthew Elbey, E-L-B-E-Y.

It seems like this problem is actually might be -- or these two problems might be a lot easier than we're talking about. If we simply attack the spam problem, in doing that, we're going to have to use reputation. When we start using reputation, we're going to be making the ISPs force their customers, either to stop sending email, or fix their computers. If we're doing that, we're going to be -- not only the botnets, but basically if they're securing their computers against botnets, they're going to be securing their computers against the other things that are phishing even separate from email.

So, maybe it's encouraging we can do both, do all of them. And then my question is, did any of you guys manage to listen to the CSV presentation yesterday or the sort of end -- do you see that as having better security than the other systems?

MR. SALSBURG: I think there are really two issues here and we will address youro the relative merits of the security of CSV versus other authentication systems?

MR. MOORE: My take on CSV is that it protects a different aspect and you don't want to be thinking of these as either/or alternatives, you want to think of them as security in depth. And so you want as many different things that compliment each other as you can get.

MS. DIWANJI: I think one of my observations from yesterday's discussion is that the way the proponents of each authentication standard are so passionate about their own standard that the audience is sitting there thinking are these exclusive or what? But they're really not. So, I would add to the comments that it seems like a nature of compliment.

DR. HALLAM-BAKER: I was thinking that maybe Carl Hutzler's suggestion of, okay, take the CSV checking, but merge it with the SPF syntax. At this point, I am absolutely uninterested in anybody proposing any other syntax than SPF for describing the IP addresses of my board email gateways. Ain't going to happen. And, you know, this fantasy of the new resource record, especially for SPF, ain't going to happen. Ain't going to be deployed. Not doing it.

add in the CSV checking, I think that would be practical, and if the CSV people submit an RFC of that form, I'm sure it will be accepted. Otherwise, I suspect that we'll make Carl write it.

MS. DIWANJI: May I make one additional comment?

MR. SALSBURG: Why don't we go to Scott.

MR. CHASIN: I would just propose when analyzing the differences between CSV, Sender ID and SPF, there were some comments that have some merits to explore. I think Douglas Otis talked about the complexity of the PRA algorithm, the complexity of a script-based, you know, credential, living in DNS, how that's parsed out, in relation to denial of service capabilities. Somebody using those records to create a malicious denial of service event high enough to source port for those EDP queries in essentially shutting down authentication.

So, I think that we need to explore that, and again, I think the tests and the direction of some of these real world test beds will help with that. And not just independent testing, but, you know, interoperability between larger mail populations, large domain houses, et cetera.

MR. SALSBURG: Pavni?

MS. DIWANJI: Well, the only additional comment that I had is just as a vendor who is trying to implement and keep track of all of these standards, it would be nice if there are three of them that are prevalent, versus 14 of them that are prevalent. So, to the extent that we are saying these are all complementary, I think it is still nice. I think there was a lot of talk yesterday about merging some of these together and I think that would on the whole benefit the community.

MR. SALSBURG: Brian?

MR. CUNNINGHAM: I just wanted to point out with your point about securing the overall system. I think that we're going to have a culmination of all of these standards, I really do, and future standards. I think it's going to be a constant moving target. I mean, the NSA has a mantra, the attacks don't stop, they only get better. And I think that's just a reality that we're facing.

MR. SALSBURG: Let's take another question. The front row, again. People who show up and are eager, in the front row get the advantage.

MR. ANDERSON: Dave Anderson from Sendmail.

So, I think this would have been vastly more interesting if half the group had been talking about attacks and half the group had been talking about defense, because, guys, the responses to most of the attacks you're talking about, the answers are almost trivial. I mean, you think we haven't thought about these things when thinking about authentication schemes?

And I'll give you an example. You know, machines, zombie machines, hey, of course zombie machines can send spam. That doesn't mean I have to read it or receive it at the other end. All authentication does is give me as a receiver a tool that allows me to go do a bunch more work to decide whether I want to read something. And so you can send it, but just because somebody's machine is infected doesn't mean that that person's on my allow list, doesn't mean that I'm going to subscribe to a reputation service that allows zombied machines to stay there with a good reputation for more than probably seconds.

So, you know, this is -- authentication is really about the user, the receiver being able to take control and manage their end of the network, not about the senders making life great for me. Senders just need to give me some information so I can do my job.

MR. SALSBURG: Scott Chasin, is there a -- is that a fair critique, or if there's a zombie network that's operating that's going through an ISP's MTA, what's the receiving --

MR. CHASIN: Sender as an organization, right, I mean, not sender as an individual. I think that's a good differentiation. I mean, zombies after infection, what do they do? And they do it really well. Is they harvest an address off your local machine. So, if that just happens to be your address book, exploiting those known relationships, quite possibly could mean exploiting know, what, safe lists, whitelists, challenge response lists. So, I think you have to look at it from that perspective.

You know, it's the massive infection means massive exploitation of known relationships. Which could have an impact overall in the future to the sophistication that's built in these networks. So, you know, it's you have to look at it from sender authentication as in an organization verses as an individual. And I think that's a -- that needs some clarity there.

MR. SALSBURG: Let's take another question. This gentleman right here.

MR. LEIBA: Barry Leiba, L-E-I-B-A, IBM research.

On the zombie issue, I have addressed this with some ISPs before, so let me start with Tripp on this and the rest of you can respond. I've discussed the idea of having in the service agreement something that says that we have a say in how your machine is configured if you want to be on our network, and you have to have certain -- you have to meet certain criteria, you have to have certain security things on there, you have to have a firewall, you have to have certain antivirus software, whatever it is, to try to reduce the ability for spam to create zombies. Can you see in the future your ISP or other ISPs adopting something like that to try to lock down the machines that are allowed to connect to your network?

configuration of a client who connects to the network through the network's integrity is preserved. That will be the private sector model that would probably have to take place here, given the lack of cohesion between the 13 offerors of the location.

MR. SALSBURG: Let me throw out a question to Tripp. Currently at the FTC when I work from home and use the VPN, I sign an agreement where the FTC administrators can scan my home computer and make sure that I have up-to-date virus settings, I assume they check for spyware, things like that. Is this something that the ISPs are considering doing for their own members?

MR. COX: You know, right now we're providing as many tools to our customers as we can, and we'll continue to do that. Our preference is not to manage a million or five million more PCs if we can avoid it. So, I think definitely providing tools is the preferred strategy from our perspective.

MS. DIWANJI: I have a comment here. I think that I cannot comment on the ISP, but we serve about 800 enterprises and when I talk to the CIOs there, you know, the challenge there is if you ask them where do the zombies come from on your network, when they appear on your network, where do they come from? You know, they all have strong policies about what is allowed and not allowed, but like one conversation I was having, said that the cycle seems to be like email, of course, and then the USB channel. And I think the challenge is not whether there are policies in place, the challenge is how enforceable it is, practically.

MR. SALSBURG: Keith Moore?

MR. MOORE: I think one effect of if ISPs start doing that and saying basically we're only going to allow you to run these kind of systems on your network, is that you're reducing the amount of diversity of the systems that are out there, and you're actually, if you're not careful, you're increasing the vulnerabilities. I mean, especially since I don't run any Windows systems, and one of the reasons I don't is because of securities risks, but if my IP says you have to run Windows and you have to run a virus software and all that, I would say you're compromising my security.

MR. CUNNINGHAM: It is a private market and you have your right to get your access some other way.

MR. MOORE: There are fewer and fewer providers all the time. And by the way, you are my provider.

MR. CUNNINGHAM: And we appreciate that.

MR. CHASIN: Just a quick comment on that. There are some interesting areas here to explore.

Especially in corporate networks, where a corporate machine could be hijacked and used as a weapon or a tool in a distributed service attack against another organization. There's some interesting questions about liability there for an entity that faces that concern.

So, I know that there are some tools that are being developed to create a network of security solutions that should be installed, or active, and then manage that at a network level. So, I think there's some validity there from a corporate perspective in looking at how to control zombie proliferation inside of an intranet or corporate network.

MR. SALSBURG: Dr. Hallam-Baker?

DR. HALLAM-BAKER: I think the good part about what you said was that we don't have to accept the Trojans and the zombie machines as a given. And step number one in reducing the number of Trojans and reducing the number of zombies, emaaTjET1.0uETticThere'1.00000 0.0

As far as telling end users what to do, though, I've, you know, the Worldwide Web, one of the origins of it came from an unpleasant bunch of system administrators whose approach to computing was you are going to use our IBM, and by the way, we wrote the operating system, it doesn't run a standard IBM operating system, it runs the one that we wrote for it.

So, I don't like that form of dictatorial system administration. If we're going to say to users, make yourself secure, we've got to make it so -- we've got to make it like a light switch. It's got to be something that you just plug in and secure. So now I don't think that the responsibility is ever on the users, it's on us as technologists and the ISPs.

One thing we could do is say, okay, if email is going to go from point A to point B, from now on, no executables go over email. Full stop. Or if you do want to send executables over email, then you must have anti-virus.

MR. CHASIN: Or put them in a zip file, right?

MS. DIWANJI: I was just going to say, next you'll be saying don't transport any message over email, because, you know, you might have -- I mean, I think it's ridiculous. I do. I do.

DR. HALLAM-BAKER: No, actually, with the zip file format, even if it's encrypted, the manifest of the zip file is not encrypted. So you can still scan for executables. And I know that, okay, there are still going to be some coming through, but all I need to do is to stop 90 percent of the infections from working and the number of Trojans that reach the end target goes down dramatically. This is a numbers game.

MS. DIWANJI: I do take an offense here. Because it's like saying, you know, my arm is fractured, since you are trying to fix it, cut it off. Even though it is useful, I do not want us giving restrictions on it like this. We can solve this problem together. That's -- it's our problem to solve and we can solve it together.

DR. HALLAM-BAKER: When was the last time you sent an executable?

MS. DIWANJI: Well, the thing is that -- well, I mean I just highlight it, right? Like people on another panel where they were talking about basically restricting people from sending JPEGS, because of this new virus that's been found. I think it's ridiculous. It's too useful. I love sending pictures to my family. You know, I can come up with scores of examples where sending an executable in a safe manner is very useful. So, I want us to attack the problem at its heart, right, not kind of say, "okay, we're going to restrict the use of email."

MR. SALSBURG: So the goal then would be to keep the utility of email, but find a way to make it so that there's less spam and less risk, efficient.

DR. HALLAM-BAKER: Look, images are only going to be dangerous if you've got a bug in the reading software. Before the Unix people invented the buffer overrun bug, and, you know, there were no buffer overruns before C invented them, you know, it's pretty easy to write code that doesn't have buffer overruns. Okay, assembly didn't have them.

MR. BURR: Okay, I wrote that one for C.

DR. HALLAM-BAKER: But, you know, executables, I don't see any reason why programmers should be sending an email.

MR. SALSBURG: Well, speaking of buffer overruns, there's a little buffet about to be overrun. So, I would like to thank our panel, and we'll see you in 15 minutes.

(Applause.)

(Whereupon, there was a recess in the proceedings.)

MS. COLEMAN: Hello, everyone. Thank you all. I hope you enjoyed the break, we're going to go ahead and get started.

We're now in the place where we're going to talk about real world effects. We've spoken a lot about some

David Lewis, Vice President, Deliverability Management and ISP relations at Digital Impact. And it's a long one, so I'll keep going.

We also have Fred Lindberg, Chief Technology Officer of CheetahMail, which is an Experian company. Then we have Peter Milla, Member, Board of Directors, Cochair of Technology Committee Council of American Survey Research Organizations. Then we have Margaret Olson, CTO and VP of Constant Contact. Daniel Park, Chief Technology Officer of Roam Secure. And last but not least, Robb Wilson, General Manager of Quris.

All right. Well, let's go ahead and get started. Elizabeth, Elizabeth Bowles, you're with Aristotle.net, that's a small ISP. Why don't you tell us how you think domain-level email authentication will affect your company.

MS. BOWLES: Okay. I actually want to start a little bit about Aristotle. We have roughly 40,000 customers nationwide, so in the broad scheme of things we're a lot smaller than the ISPs you heard from today, but we're also a lot larger than the other 590 ISPs that are in Arkansas that this is going to have a significant impact on, and we call those the mom-and-pop ISPs, and I think for them, whatever you hear from me you can multiply that for the ones that are smaller than we are.

Aristotle has been very active in the fight against spam. We have been very aggressive in trying to stop it coming into our network, trying to prevent it getting to our customers. As an ISP, and that's all we do, and as a smaller ISP, we don't have sideline businesses, we don't have affiliate networks, we don't market to our customers. So, all we really care about is what our customers think is spam. We get a lot of complaints from our customers about spam and every step we have taken has been to try to reduce the flow of spam into their mailboxes. Particularly malicious spam or things that can harm them.

We take our role as an ISP extremely seriously and we do think that it is the obligation of ISPs to be at the forefront of this industry because we're in the best position to protect the consumers. Consumers cannot protect themselves and we have to do it for them.

So, here's what we already do, and I will go through this really quickly and I will get on to the important subject. We do port blocking, we do rate limiting, we do monitor our networks for spikes to see if people are using a zombie. We have service agreements in place that allow us to cancel accounts immediately, charge penalties if people are spamming across our network. We have a spam and virus system.

One is a reputational system that sits outside of our servers that identifies spam streams or if it looks like it's a zombie computer, we will stop it before it ever hits our network, and then we have a content system that does the typical type of spam filtering based on baysien stuff. Thanks.

That way, we actually eliminate 99.9 percent of spam. So, our customers get virtually no spam. It doesn't mean we don't. We get a huge amount that we never pass on to our customers. So, we take our responsibility very seriously. If our customer has a problem with their computer, they can call us, they can bring it in if they are in Little Rock and we will fix it for them. We do have customers nationwide, we have customers in all 50 states, but the bulk of our customers are in Arkansas.

Okay. That said, we think that any email authentication system has to be a unified standard. We, a few years ago, or about a year and a half ago, we decided we wanted to try reverse domain look-up. We thought, okay, if we reverse the DNS, we are going to be able to see if the person is actually who they say they are and we are going to be able to eliminate a lot of spam by blocking it before it ever comes in.

The problem was, a lot of mom-and-pop ISPs and a lot of businesses, as a matter of fact, don't really know how to configure their mail servers to deal with that type of a query, and as a result we had a lot of complaints who couldn't get an email to their aunt in Hoboken and we had to turn it off.

That's why the standard has to be unified. We can't have AOL implementing one standard and Microsoft implementing another and everybody having to comply with a bunch of different standards. It really does have to be unified. And I think everybody who I have heard in the last day and a half agrees with that.

I also think it has to be easy to implement. I don't think it can have any piece of it that is proprietary that would require us to basically get a license to a piece of software that we couldn't subsequently modify or improve. If it is proprietary, I think it needs to be open, I think it needs to be a flexible system, and that is really important. We're not based on a particular platform, but a proprietary solution would not be appropriate for us, and so we think it has to be an open standard.

We think moving in steps is great. Moving all of this is marginal. Nothing we've talked about today is going to prevent us from still having to do all the filtering we do. It's not going to decrease the flow of spam, per se, but if it is true, as one of the panelists said yesterday, that the seven percent of the ISPs who particularly think was positive. And we believe that what our customers think is spam is spam, they define that as any email they don't want to receive, and trust me, we definitely hear about it if they get it.

Let's see if there's anything else I wanted to say. I think that as the last panel pointed out, there is no one single silver bullet. I think that CSV is something that definitely merits looking into. Like I said, we are going to look at implementing SPF immediately. And as far as DomainKey cryptography, we're not going to look at that. That's something that would -- I mean, we will look at it in the sort of in the background think about this later on, but there's no point even trying to do that now in our position because there isn't enough industry-wide buy-in for that to be something that we could feasibly do.

MS. COLEMAN: Great. Well, thank you, Elizabeth. You've mentioned a couple of interesting things about the need for a unified standard in your view, the desire to have the standard be one that's easy to implement.

Arthur Emerson, you are also a small ISP in your own description. Do you have anything to add to Elizabeth's remarks?

MR. EMERSON: Well, my particular concern is in the implementation, because I have a staff of two and one of us is in Washington, D.C. today, and the other person has been working for me for about a month and a half, so he is on his own today for essentially for the whole week.

I just brought along this book here as a prime example. Everybody recognize it as a bat book? This is edition number one, 1993 and it has 804 pages in it. If you expect, any time you need to configure sendmail to do anything, you have to open this book. It's been well worn in my office. I happen to have a copy of it. I know plenty of ISPs who are running sendmail that have never even heard of the bat book. It's just a big concern.

At our college, we have about 2,200 users, 250 faculty, 850 resident students, and some of the measures we've taken is we've actually blocked Port 25 for everybody. We will not allow any student computer access to Port 25, even to our internal mail servers, they only have web mail access, to add an extra level of insulation to it.

We've published our SPF records since July. Another concern is purchasing cycles. For the college, I just had to submit last week my purchasing recommendations for equipment I need for July 2006. If we come up with a proposal today that requires me to spend one dime of money, I don't have it until July of 2006 to buy equipment or software to bring this up, which is a major concern. It's a huge hurdle to implementation in academia and other areas as well.

And one of our areas that we're unique in is that we have an elementary school on our grounds that we provide Internet access to. There are all kinds of federal regulations involved, we've given children Internet access, and we wouldn't dare give them email access, because I just don't even won't to go there, but they have requested it.

MS. COLEMAN: So, it sounds like you have some unique problems. You mentioned in particular your purchasing cycles. I wonder, Elizabeth or Arthur, would either of you like to talk more about cost issues?

Elizabeth?

MS. BOWLES: Well, our cost issues are kind of -- we are in a little bit of a different position because we charge a metered rate. We charge 50 cents an hour and only for time online. So, we don't have a huge margin that we can bet against, or raise our -- what is the phrase, raise our net cost. We can't raise our bottom line too much, because if we do we're cutting into what isn't that great of a profit margin to begin with. I mean, we have a good profit every year and we're a growing company, but we can't -- because we're a metered rate, we can't afford to implement a solution that would cost us another $150,000 to do. But that's why SPF is so attractive because we have a fixed cost on that and that is nothing.

And when -- if we have to upgrade to Sender ID and that's going to involve our having to upgrade our spam filter because they're going to have Sender ID authentication in their spam filtering, whether we do that is very much going to depend on how much that costs, and if it is any significant amount we really won't be able to do it.

We don't pass costs on to our customers. When we upgraded our spam filtering system a year and a half ago, we bore the entire cost of that and it was significant and we don't pass it on to our customers and we wouldn't pass it on to our customers here. So, for us the cost is a very real issue.

MS. COLEMAN: Wow, that's great. Thanks Elizabeth.

Arthur, did you have anything to add about the cost issue?

MR. EMERSON: Yes, I did. First of all, the college is not in an urban area. We have a T-1 connection and we are actually buying tiny megabits of fiber for our students, but even a T-1 connection out in the rural areas we're in is not cheap. So, any increase in bandwidth to validate email coming in, it is a concern.

Also, a multiple standards, I mean it's multiple resources. So, if we have to adopt all these different standards that were talked about today, it could be 60 to 70 percent CPU utilization increase, and I'm looking at needing a server no matter what, that hasn't been budgeted for yet.

Purchasing cycles we discussed. I also just today, thinking about it, we need a DNS cache server, because if we're keeping 512 byte keys in memory, or 512 bit keys, we're going to need additional DNS cache that our current DNS servers are not set up to handle. If we need the paper certificates or some other si.00r I a.42If we

Association. Tell us about some of the concerns that you may have.

MR. GRECO: Well, first of all, good morning, and thank you for having us here today. I think I can safely say that we represent a unique perspective here at this summit. I believe we're the only organization that really does represent both the marketers as well as in addition to the service industries who support them. So, when we cut across it, we're really looking at representing the entire value chain of direct and interactive marketing.

And so this is a very, very important subject to us. I can't imagine anyplace I should be today other than here, because we really look at this as protecting brands and really protecting consumer fraud. We are fighting a war. All right, I think if we think of it as anything less than that, we're making a huge mistake. All right, in terms of a war that's really protecting legitimate emails, and legitimate commerce that's conducted through email.

So, as I think about this in terms of real numbers and the reality of consumers and the way they're interacting with businesses, we've got research that demonstrates $33 billion in sales last year were conducted through the legitimate email channel. And when I say legitimate, I'm talking about books, clothing, travel. Things that all of us in our homes and our families use, and count on being able to keep that channel wide open.

Maybe even more importantly, when we think of where the growth in the economy is coming from, email marketing is extremely critical to small businesses. Of that $33 billion, $8 billion in sales were really as a result of small business interaction and dependance on email. And if you really think about it, small businesses must depend on email, actually we found at a rate twice as high in terms of the percentage of a large business, because they don't have those customer relationships, necessarily, so they have to reach out in order to grow their business.

So, if we want to continue supporting the growth those who they are not, with the consumer, and confusing the consumer.

If we're at war, and we carry that metaphor out, then we use every weapon at our disposal, and we start using them now. All right, and so we believe very strongly, and that's why we've taken a leadership position here with this industry, we've been continuously educating our members. We've had the Webinars that started last August, we're going to continue them, we're going to have another one on November 22nd to brief our members on the outcome of this forum, and the purpose of that is we've been encouraging our members all along to comply with both standards that exist, whether it's Sender ID or SPF.

We in our own organization have done that, and our technical organization has assured me that in their case it only took them about an hour to make sure we were in compliance. So, the issue here is not that this is that technically difficult to do from a business perspective, the important thing is that we get everybody moving forward with the tools that are identified today. Probably my greatest fear is that these two days could result in paralysis by analysis in terms of where are we.

All right, if we're going to be moving forward, we've got to be moving forward with the tools we have. They may not be perfect, they will continue to evolve. The people who are the technical experts in this room know far better than I do that technology will continue to evolve, and that anything that we discuss here today, if we come back three months from now, there will be another spin on it, there will be another twist on it, there will be another advancement made. And while we're watching that evolve, I think it's imperative, imperative that we move forward with absolutely every tool that we have at our disposal.

Now, I do agree that the bottom line here, though, is that the tools that are implemented, the discussions around whether it's one standard or multiple standards that peaceably co-exist, the issue is they have to be easy to install and use, they have to be low cost, we have to make sure that every business that needs to communicate with consumers has an ability to easily implement this, in a low cost way.

MS. COLEMAN: Thanks, John. Sounds like you have some similar concerns in terms of ease of implementation and ease of use. You started out talking about small businesses, and some of the differentials there.

Margaret Olson, you are with Constant Contact, which actually is a web-based email marketing service that enables small organizations to build and manage permission-based email lists. Can you just tell us a little bit about your perspective in all of this?

MS. OLSON: Sure. Constant Contact, as you mentioned, provides email marketing to the small and medium-sized businesses. Most of these people have lists under a thousand. They are using mail to continue their relationships with their customers, in what is really the most cost effective way for a small business today.

When I -- I personally have been very active in the efforts to combat spam, participating in many of the authentication efforts, because from my customer base, this is incredibly important. Small businesses tend to -- they don't have brand names, they don't have a huge reputation, their customers know them, but when you look out at what happens today, spam is definitely a war. Small businesses, unfortunately, are all too often collateral damage. Because they don't have the bandwidth to deal with the kinds -- unless we do it for them, and to a great extent we do it for them, but when, you know, something inappropriate happens on the receiving side, someone has to go and talk.

So, when I look at authentication, I think, authentication coupled with accreditation is exactly what my customer base needs. They need a way to say, I really am Joe's Bicycle Shop, and you, ISP, can accept this mail and know that it really is Joe's Bicycle Shop. And authentication is the first step on that road.

When I look out at, you know, some of the details of the proposals we've seen, and the discussion about how small businesses are going to implement them, I think, we have a little ways to go. It is one thing to say, you know, run this wizard and update your records. Well, most of my customers don't know what DNS is, I doubt they know who their DNS technical administrator is, and those wizards are aimed for -- at -- wizards, yes, wizards. Right?

It needs to be something that says, you know, I use Aristotle for my person-to-person mail and I use Constant Contact for my marketing mail and that's it. And I think that when we have a number of competing standards, that makes that whole process more difficult.

You know, at the end of the day, Constant Contact is going to implement them for their customers, and if it's four records instead of two, I don't really care, to tell you the truth. But I do need my customer to be able to understand what piece of information they need to gather and who they need to tell it to. And because from a technical point of view, they're consumers, right? They know about as much technically as your average consumer does, and they need that level of tool.

MS. COLEMAN: Okay, great. So, again, it sounds like ease of use is going to be a big issue for you. If you can't click a button, basically, it can cause some problems, Margaret?

MS. OLSON: Right. You have to be able to click a button.

MS. COLEMAN: Okay. Well, we also have Dave Lewis with Digital Impact. You're also in the business of using email for direct marketing. How do you weigh in on this?

MR. LEWIS: Well, we're kind of at the other end of the spectrum from Margaret's company. We deal principally with large financials, retailers, those in the technology industry, travel and hospitality, brands that you would recognize that are principally Fortune 500s, like Wells Fargo and MasterCard, and Fidelity, and Country Wide, Gap, Victoria's Secret, Marriott, those kinds of companies.

Our challenge is that while we may be able to publish our SPF records for the strong ends, many of them are using branded domains or vanity domains through us that creates challenges. Plus they're mailing also on their own side. It's not that they're mailing exclusively through us. They're also mailing in-house, and for a large company just trying to figure out what are the various domains under which they send is a major hurdle.

You know, I would like to just step back and talk a bit, if I may, about how we see the broader issue, because Digital Impact has been around this debate for quite some time. We are a charter member of the ESPC, that Trevor heads, active on all its committees. I co-chair the one that evaluates reputation systems. We were active in the original blueprint that turned into Project Lumos. So, we are very much behind what this is all about today.

We very much buy into the idea that we must establish authentication and email accountability, and that the two must go hand in hand. And step one is to identify the sender, step two is to hold that sender accountable for their practices, and accountability means impose a cost. And that cost can be direct in the form of a postage stamp or a bond or it can be indirect in the form of, you know, denied access or poor placement. But the point is, to hold mailers accountable. Hopefully they are going to be the spammers that we hold accountable and deny access to the medium.

But, you know, I'm concerned that on that second point is that we've got a long ways to go to bring along those in the direct marketing industry, and although my title is ten feet long around deliverability and ISP relations, I'm a 20-year direct marketer, offline and on, and so I bring that kind of perspective to the issue.

From my perspective, what really is important that we understand here is that we're losing consumer one, which is really what's going to start addressing the problem, and that's accountability.

So, you know, as I look at the various debates around should it be SPF or Sender ID or whatever the heck it is, there's a couple of points I think. One, it's not a sender/receiver issue. Yes, we're going to do as an email service provider whatever it takes to get the mail delivered for our clients. But that's not the point. There's a lot of other companies out there that are trying to do it themselves. You're looking at a very decentralized, highly fragmented environment with, what, millions of senders, 500,000 domains around the world that accept email. It's going to be tough enough just implementing one likely standard. Okay? Put the heavyweight standard around cryptography aside for a second and just focus on the lightweight.

And I say the points made earlier about a single standard are important, but let's define what single standard means. For me, as a sender and a representative of the sending community, it means I really don't care how many different ways you intend as a receiver to interrogate the record I publish. Do whatever you need to do to ensure that you're getting the right kind of mail into your domain that your members want. But don't ask me, or mailers in general, to publish more than one record. Knock off this debate about version one or two. If version two is the best record available, then publish it. Make us publish it. Ask us to publish it. But do it now, before all of us get too far down the road in terms of implementing just version one.

The reason that's important is if you don't do that, then we're not going to get adoption in the center community, and we need adoption. We need it badly. We need every sender out there to be publishing their records, because if we don't get adoption, what's going to happen?

Carl Hutzler can't make the decisions that he needs to make at AOL on the basis of authentication, because he can't tell the difference between somebody who's misapplied the rules or hasn't applied them or is spoofing him, but probably more tragic than that, we can't take the second step, we don't solve the problem, consumer confidence continues to erode in the medium, and communication is used as a viable communication and the vehicle for communications in commerce goes down with it. And that's what my main concern truly is.

MS. COLEMAN: Wow. Thanks a lot, Dave. Sounds like some of your concerns are that if this isn't done in a unified way, such that you all don't have to publish more DNS records than you have to, that there could be a problem in terms of us getting over the hump and solving this problem.

MR. EMERSON: It just contributes to the confused environment that we all know that spammers thrive in.

MS. COLEMAN: Fred Lindberg?

MR. GRECO: Excuse me, Sana, I've got to respond just to one comment that Dave made here just to clarify something, because he talked about the direct marketing industry and the status of it and I think I would be very remiss if I didn't make clear, extremely clear, that the direct and interactive marketing industry that I represent, which is 5,200 members throughout every part of the industry, are number one, responding very positively to our direction to comply with these standards, but more importantly, we have an extraordinary effort in terms of our ethics and privacy and policy issues, our marketing practices committees, we self police the industry, we self regulate the industry, we remove members from the association and remove their benefits from them in terms of participating in the association.

And so I think the industry is way down the path in terms of policing itself. It's those who are outside of the industry, the smaller number of "bad guys," as we know it, who are creating the mass problems that we're all here trying to attack.

So, again, I just want to make it very, very clear that we continue to make sure that we have the appropriate ethics and policies in place for the community that we represent. Thank you, Sana.

MS. COLEMAN: And Dawn Rivers-Baker, did you have something to add?

MS. RIVERS-BAKER: Yeah. As long as we're talking about small businesses here and as long as we're talking about this entire system that we're setting up, I think that one of the things that has become very clear to me listening to people in the last day and a half or so, is that there seem to be a lot of people working on designing the system who don't have a real clear idea of how real people use email.

Our members, a lot of them have multiple domains. They do not necessarily have the resources to lease service space for each one of those domains, so that they have redirects in place, and they have mail forwarding in place. They have payment processing systems that send out email receipts on their behalf from their domain names, and all of this stuff needs to be taken into account when you're designing these systems.

While we're at it, we need to talk about the rest of the system, not just the authentication, but the reputation and the accreditation, because when it comes to our members, and our members are really teeny, teeny, tiny small businesses, International Council of Online Professionals, it sounds really pretentious, but it's really a bunch of very tiny small businesses, a lot of them are run on a part-time basis. A lot of them are home-based businesses. They don't have a lot of money to work with. They don't have IT staff. A lot of them do their own IT work because, like many small business owners, a lot of them are control freaks, so they want to try to do it themselves instead of hiring it out.

And as a group, we have been getting slammed by the spam issue from every direction for a really long time. Because we have to maintain a public presence online, if your average consumer is getting 100 pieces of spam a week, we're getting about 300 a day. And we don't have staff to wade through it, so we have to do it ourselves.

At the same time, my web hosting company recently implemented a spam filter, and it was really great, because it reduced the level of mail I got immediately so that the stuff that I was getting from

newsletter that week. We've got situations where that you tell us to jump through. You want us to publish 57 records? We'll do that, too. You want us to encrypt? We will do that, too. You want us to tango? We'll tango. You want us to Charleston? We'll Charleston. We'll do whatever we have to do.

But at the end of the day, if we're still going to be in a situation where we are being held to a standard and we are holding up our end of the bargain, and bad-tempered consumers who forgot that they subscribed can ruin our reputations, where does that leave us? Still unable to get our mail through. That's not going to work.

There needs to be some mutuality of responsibility here. Because if we're going to play by the rules, and still get shafted, that's -- then you're driving people out of business and off the map. And that's not what we're here for.

MS. COLEMAN: Well, thank you, Dawn. It sounds like you've identified a serious problem. You want to be differentiated from the spammers, and it sounds like you think authentication will help with that.

I wonder if Fred Lindberg, who is with CheetahMail, I wonder if you would also agree that authentication is going to be a solution for that problem for you as well.

MR. LINDBERG: Yes, I definitely agree. I wanted to first thank the FTC and NIST for convening this summit and Sana Coleman for chairing the panel and allowing CheetahMail to participate here.

We have a slightly different situation in that htl16wantkenow why not firspublish multiple of panse recha deTjET1.0000 reputation.

So, we can work on our clients based on their reputation. What they do affects our reputation, which means it affects our costs. And what we do, and what our clients do, affects our reputation with the big ISPs. And at the moment, more than half of email from our clients that our clients send through our services go to big ISPs. So, why not start testing this and doing this? I don't think there needs to be wholesale adoption up front. There are very easy ways to test this, and we can help and contribute.

It will help our clients, but it will also help shake out which of these solutions work well. There may be solutions that work much better for us than for somebody else. So, for us, the Sender ID, SPF and tying that to a client domain is very easy, because clients delegate a sub domain to us. We at CheetahMail can manage their authentication and their email, we can give them private IP addresses, we can do all these things.

The difficulty comes in when you start to have many more, as we heard, many more smaller clients, where it is hard to work up front directly on their reputation. You have to work on the ISP's reputation to some point. And when it comes to zombie networks, obviously it is an ISP reputation, because it is in the end the ISP who can do something about the zombies.

MS. COLEMAN: Great. Thanks, Fred.

Trevor, we've heard from Dawn that she's willing to do all kinds of dances and we've heard from Fred that he's willing to be a guinea pig. Why don't you tell us how the Email Service Provider Coalition feels about all of this.

MR. HUGHES: We're willing to be dancing guinea pigs I guess. We -- let me tell you a little bit about the Email Service Provider Coalition to give some context to what I am going to say. We are an organization of 52, not surprisingly, email service providers. And email service providers are companies that help other organizations deliver their mail.

By just a quick run through our membership, we estimate that we deliver mail on behalf of 250,000 senders in the United States, many of John Greco's members, many of the folks in the room, actually, probably deliver through one of our members.

Our friends at IronPort, through SenderBase, have done some analysis and they estimate that on -- in a total look at email going across the Internet, we are responsible for about 12 percent of that mail, and if you take out spam, we're responsible for about 25 percent of email that's online today.

So, we really see an enormous swath of what is being sent and received out there. And we don't just represent a marketing perspective, we actually represent the full breadth of email communication. Many of our members do deliver marketing messages on behalf of their clients. Many of our members deliver transactional messages, shipping confirmations, purchase confirmations, newsletters.

We have some members that are incredibly niche focused and just provide newsletter delivery services. So, we really see the full breadth of email communication.

Now, when we were formed some two, two and a half years ago now, we really saw two distopian visions of the future. We saw two enormous problems that were facing the email world. On the one hand, we had spam, and phishing was very early at that point, but we had spam primarily that was really undercutting the trust that consumers had in e-commerce and in the online space, but it was also crowding the inbox to a point where it was becoming so littered with junk as to be not as functional for legitimate purposes.

And we saw that as a clearly bad vision of the industry and we wouldn't have a trade association, confirmation, or you're sending a monthly account statement, a phone bill perhaps. False positive rates in that channel, in that area, again we see the full breadth of email, really creates a challenge that I think can call into question the investments that have been made into email and e-commerce generally.

I'll give you a couple of examples of false positives. Actually, I'll give you one example of false positives that I think is pretty funny. When I submitted my request to participate from our domain at our offices, we use RoadRunner, which is a Time Warner property. We submitted it to the FTC, the FTC happens to use a blacklist, and lo and behold, that week, RoadRunner was blacklisted. So, I got a bounce back message from the FTC saying that our request to participate in the Email Authentication Summit was not delivered because RoadRunner was being listed on one of the blacklists at that time. That's a very real example of a false positive. And that's the type of problem that we've been working on.

So, we came together as a trade association to try to address both of these problems. We wanted to try and insert into the middle of those two distopian visions an idea that legitimate email really deserves a voice, and that it is important and that we should protect it. And we started talking early, early, early, about, well, how do we protect ourselves? How can we create the best whitelist that there is out there. We know that our practices are legitimate. We know that we are desperately trying to do the right thing. Let's create a whitelist and give it all the teeth in the world and if someone violates our standards, we will kick them off and then we will go to the ISPs and say please take this whitelist and deliver this mail, because we're really the good guys.

The more we talked about that solution, and this was early on in our technology committee, the more we talked about it, the more we realized that it solved the immediate acute problem that we had, and that was deliverability and false positives, but it did not respond to the larger chronic problem that we had, and that was spam. That spam was going to continue growing, and while we may win that battle, we would probably lose the war in the end.

As a result, we stepped back and we said, well, what's fundamentally wrong with email and what can we do to address it, and we came back to accountability. We kept coming back to that word, over and over again. That email really allows for the impunity of anonymity, that you can spoof who you are, and therefore not be held accountable when you send email. And that anonymity allows for a lack of accountability. And so we started to talk about solutions that would drive accountability.

That led us to some 18 months ago now publishing something called Project Lumos, which was our best thinking at the time on how do we build accountability into the email system. There were a number of components to it, authentication, accreditation, reputation, enforcement, and Margaret Olson from Constant Contact and Hans Peter Brondmo from Digital Impact who you will hear from later this afternoon were the co-authors for Project Lumos for us.

We still see that as a compelling vision for how we can move towards a better solution towards spam and a better solution towards the collateral damage we see in the marketplace. Now, since we released Project Lumos, we actually envisioned an encrypted solution for authenticating email in Project Lumos. Since that time, we've been very active holding meetings at Harvard Law School in January of this year, participating with Microsoft with Sender ID retreats out in Redmond, and we see now that we really need a phased approach. That the challenges of implementation really demand that we move with an IP-based solution first because it's here and it's now and we can act upon it immediately. And yes, there are criminal elements out there that may try to subvert that system, but you know what, there are benefits, too, and those benefits outweigh those potential costs from criminal activity. And regardless of what solution we put together, that criminal activity is going to exist, no matter what.

So, we are really supportive of, and in fact now require our members to be publishing SPF records and are looking forward to having all of our members publishing Sender ID records hopefully by the end of this year. We have been very active in educating our members on this, we have been very active in engaging with Microsoft and with Meng on these solutions.

At the same time we have been very active with the encrypted solutions, and again, it was part of our original vision and will continue to be. We see that as the next step for us. That we need IP-based solutions now and encrypted solutions down the road.

So, let me just throw out a couple of challenges that I think we have, and we've heard a little bit about implementation and the willingness to dance, the willingness to be a guinea pig. I think a lot rests on the ISPs' shoulders right now. I can attest for the sending community and say that we stand prepared to implement just about whatever authentication scheme comes forward, but it's really up to the ISPs to help us make that happen.

And I think we need a carrot and stick approach here. I think we need a carrot, and that carrot is deliverability. And the ISPs need to offer, maybe it's not dispositive of inbox placement, but they need to approach now rather than crypto-based approach. Is that because that's -- is that because the industry is farther along in terms of defining the IP-based or do you really believe that works better? Why is that first?

MR. HUGHES: Well, so it's actually not one before the other. I think that IP-based solutions are here now, and we require SPF records now and are looking forward to Sender ID records being published by all our members very soon. At the same time, we actually have some members, SKYLIST of particular note, who are already publishing DomainKeys records.

So, we are seeing these in parallel, not as serial tracks, but in parallel. So, we will continue to pursue both. I think it's important for us to keep our eyes on that ultimate prize that an encrypted solution is a more complete solution for us. However, where we stand today in terms of implementation, IP-based solutions are here, they're now, and we just have to do it.

MS. COLEMAN: Okay, okay, great.

Now, Peter Milla, you are with CASRO, and that's the Council of American Survey Research Organizations. Trevor also mentioned some points about deliverability and the trouble with false positives. I would imagine

problem for us. We are seeing -- member companies are seeing real spam blocking problems. Where it's, you

know, industry-level adoption could really have an impact of knocking 90 percent of the stuff out very, very quickly.

I see that the industry needs to be -- the marketplace needs to get together on working in cooperation with federal regulators. I think that optimistically, perhaps in a nine-month period, we could have something in place that could really, you know, make things go away. I would echo the comment I heard earlier about, you know, we don't want to, you know, get paralysis by analysis, because, you know, a more pessimistic, you know, scenario might be six to 12 months to develop, come to agreement, another six to 12 months to implement. I think that we can -- that we can get there much more quickly.

I would echo some of Jonathan Leibowitz's comments earlier today about, you know, have the private sector really drive us because in the words of one of my old bosses, the solution that you devise is going to be far preferable to the solution that I impose upon you.

Again, I believe that gBT36.0000.00000 0krllechemt pla2gt

23montwilltbeI cert I .80 268izat the indue ildoers verve mucechemt pla2g and if we don't address it, in my industry, which I can speak about as my perspective, I could see that this replacement technology could really be challenged and, you know, and become obsolete.

MS. COLEMAN: Okay, great. Thanks so much, Peter.

You know, it seems like from everything we've heard, authentication, we definitely have a positive outlook about it. Now let's explore why. I would like for Robb Wilson to tell me the worst case scenario. If an authentication standard isn't adopted, what is that going to mean for some of your clients?

MR. WILSON: A large number of our clients have really moved their business objectives and the way they've done business from an offline method to an online method. So, a large percentage of our customers and clients are financial services. So, they've really removed the offline component of their business to online.

And the eroding customer confidence in email or about trust with your financial services companies. They can't -- they can't go back to an offline mode, it's really not an option for them.

So, what they're really looking to us to answer is what do they do to make sure that their messages get through. They'll do anything, to repeat what you've heard. They'll do whatever it takes to make it happen. But they're really not getting that answer. The different ISPs have different methodologies on how they would like us to guarantee that, you know, we are a legitimate sender, but it's difficult to communicate with them. It's difficult to actually itemize those out. It's difficult to keep up with them.

And I think ultimately when it comes to spamming and phishing, the people that are doing it that are profiting from this are moving very quickly. I mean, if they have an idea, they just try it and see if it works.

I think SPF and sender authentication, Sender ID are all ways to just get the ball in play, and I think ultimately that's really what needs to happen, we need to get the ball in play so we can start sort of reacting.

MS. COLEMAN: Well, that all sounds good.

Now, Dan Park, his business is a little bit unique, he's with Roam Secure. Dan, why don't you tell us what will happen if an authentication system that's ultimately adopted, if it fails. What happens from your perspective?

MR. PARK: Thank you, Sana. Thank you, FTC, NIST, and everyone who has attended this summit.

Yes, we are in a slightly different position here, I not only represent Roam Secure, but also all of our customers. We have a product called Roam Secure Alert Network and it's a merge between communication systems that's used by first responders and all agency staff and public systems.

I am not sure if people here are familiar with the Arlington alert system or the D.C. Tech system which have been launched in those two jurisdictions, but these systems are owned and operated by our customers, and the type of messages that are being sent out are of an emergency nature and sometimes can be life and safety.

And so, we are very concerned with what's going on here, because if there's any potential for these messages to be delayed or even hindered ultimately, then wireless carriers, as well as home networks and small companies, because we're hitting such a vast array of systems and gateways and filters that are in place, it's a very difficult field to look at.

The two -- I have a twofold concern, really, and one is where the messages will be hindered or delayed or ultimately undelivered, and also authentication and spoofing. We have actually put into our system a way that users can log in back to the server and see if a message they received on their email or their device is an authentic one.

We have also looked at prototyping digital IDs. And because we work with our customers to employ these systems on-site, we actually have a lot of power over how they are going to install these systems and we recommend how to set up their DNS records and other networking requirements. And so we are welcome to adopting and advising on whatever types of email authentication solutions are going to be the standard or what multiple ones will be put in place.

And so right now, we're not willing to do any kind of dances or be guinea pigs, because we can't afford for anything to happen to these types of messages.

MS. COLEMAN: Wow, that's great, thank you.

Now, Mr. Philip Hallam-Baker, we've heard a lot today about the potential burden of costs, the administrative burdens. We're hoping that this will improve deliverability, and we've also heard about the concern of having to publish multiple DNS records. These are kind of -- it's a collective analysis of what I've heard so far.

The big question of the day, if I can ask it on behalf of consumers, is, you know, the real world effect I'm concerned about is at the end of the day, will an authentication system really reduce spam and stop phishing?

DR. HALLAM-BAKER: Thank you, Sana.

I think that an authentication solution by itself will not stop spamming and phishing. It's like traffic. You have a license plate on your car. That doesn't stop you from driving too fast. Putting a license plate on your car will do absolutely nothing to it. The thing that stops you from driving too fast is your driving license so that when the cop stops you they know who you are, and the traffic cop and the courts and the fines that they can impose.

So, it's a threefold strategy of authentication, accreditation, and consequences. So, you need all three of them together, I believe can start to shrink the problem. We'll start off by dealing with the quasi bad actors, the ones who are okay, they're doing this spam because they read in the New York Times three years ago how lucrative a business it was. And we will shrink them down, and as we, you know, initially, we will start to see the spam getting nastier, because it will be the less aggressive members of the spamming community that will drop out first.

But over time, we're going to establish accountability. And people have been mentioning accountability. The thing about the tango that Dawn was prepared to dance, at the moment, if you're sending email, you're forced to dance a tango and the steps are being called out by contortionists.

And quite often, I get the feeling with the blacklist community, the real point is not stopping spam, it's showing how important they are and showing that they're the people who write the rules. And the reason why the blacklist community has utterly failed is that they demand accountability and they do not accept accountability in return.

The thing about the new accountability system that we can have in place, based on authentication, is that each component in the scheme is held accountable. The end user, the senders are held accountable, because they can be identified. There's also a very important accountability mechanism in place for the accreditation authority. If I'm providing accreditation, then if I am lax in the accreditation I impose, then nobody is going to trust the accreditations I issue.

If, on the other hand, I am arbitrary and force a contortionist to tango, then nobody is going to buy accreditation from me. So, I am forced to be accountable by both sides.

And just to -- one final piece on the cost, to get this thing jump started, we need a baseline accreditation system. One of our businesses is issuing these individual SSL certificates that we've been issuing for many years and labeled online commerce. So, one of the things we've done is we took the list of all of the domain names that we issued the SSL certificates for, we created a thing called verify domains list, and that is now available at no charge to any antispam company or large ISP, or somebody else who can give me a good reason why they should have it.

We will eventually be publishing it in realtime over DNS, so that people can look up in realtime. But that's something that we've got out there. The data has already been collected. We won't be charging for people to read it, and hopefully that can jump start the

with in one way or the another or someone in your family does business with every day, over 80 percent of them are actively engaged in interactive marketing, and if therefore if they move forward with adopting authentication, it's a step in the right direction.

And so, again, I just want to encourage us to move forward with what we have, while we continue to analyze what more we're going to do in the future.

MS. COLEMAN: Thank you, John.

Dawn Rivers-Baker?

MS. RIVERS-BAKER: I think as we talk about implementing these systems, it's really, really important that we maintain open communications with all of the stakeholders involved. I can tell you that from the perspective of most online micro businesses, this conference right here is probably the first time that they feel that the particular groups of people who are represented here have actually lent them an ear while they have been hammered by this problem for several years now.

I also think that it is important as we look at the accreditation issue, several of the currently existing accreditation services are not going to be appropriate for these micro businesses because, frankly, they don't have the money for them. There are some of them who require fees on an annual basis that are about as much as these little businesses make in a whole year. The market is going to address that issue.

ICOP is now, for example, putting together a trusted email center program for our members that will serve as an affordable accreditation service for them. It is going to be important as the market for these accreditation services for these smaller businesses develop, that we don't have the club of dominant market players online slam the faces and the doors of those new businesses so that we can't get our own accreditation services recognized and can't get our mail delivered because the big boys like to hang together.

I also think it's important that on some level, again, end users need to be held accountable so that they -- so that we are no longer operating in an environment where it is okay for somebody to be mislabeled a spammer because they've got an ex-girlfriend with a grudge.

I think that spam complaints need to be investigated on some level. I think that when people are listed on blocklists or otherwise labeled as a spammer, they have an opportunity to defend themselves instead of not finding out about it until they try to send out their newsletter. I think that someone, possibly even the FTC in the context of its discretionary rule-making authority under CAN-SPAM should develop some kind of a standard of confirmed consent and possibly, you know, single opt-in, double become aware that at least in the short run, we need an IP-based solution.

All of us who send large volumes, we can do a dance, I think, online professionals can do a dance and a jig, and I appreciate that AOL and others are going to test, but when you look at the -- most small businesses are B-to-B services. They're lawyers, right? They're not going to be doing a dance and they are not sending to the -- necessarily sending to the major ISPs.

Many, many, many of my customers do not have anything approaching, you know, 50 percent to the big three. It's maybe two percent. So, I sit here and I hear the expense concerns of small ISPs protesting this and I think, we need to have everybody who receives feeling -- with a solution that they feel able to test so that we can get the experience with the accreditation and reputation that, as Dawn has pointed out, is so important to small business.

So, you know, I think it's important to get the entire spectrum involved in the testing and the experimentation, and that, I think, at least in the short run, from everything I have heard, says that we need to start with an IP-based solution.

MS. COLEMAN: Okay, let's open this up. Do we have any questions from the audience about all of this?

You, sir, in the front row.

MR. JUDY: The name is Emory Judy, J-U-D-Y. I'm with a law firm here in town, but more importantly I'm with a group at the ABA that is looking at these issues from the lawyers point of view, and Elizabeth is in the same group.

There's two issues that concern me. One is this reliability issue and the other is whether there are any hidden dangers in partial implementation. You know, we think about it from this point of view: Law firms are under an ethical obligation to communicate with their clients on a regular basis. And increasingly, and with the encouragement of the government, law firms are doing all of their filing with courts through electronic systems. And lawyers increasingly are drafting their contracts in such a way so that all of the notices that go out under the contracts are delivered electronically. In fact, the contracts are formed and signed electronically.

In a world in which these notices don't work, there's a loss of reliability, that whole structure fails. I want to make sure you understand that that dimension of the legal system is actually compromised by these problems.

The other point that I want to make, and I don't understand this particular area, and I'm not sure it was fully addressed here, what happens in a world in which because of the huge differences between the micro businesses and the huge businesses, you see very differential levels of implementation. It's not just that the standards are different, but some people have it and some people don't.

Are these systems then -- are there communications breakdowns among them simply for the reason that you have these differential deployments, and if anybody who has a comment on that differential deployment issue, I would like to understand something more about it. Thank you.

MS. COLEMAN: Thank you. Dave Lewis, do you have some remarks?

MR. LEWIS: Yeah, a couple. I think the first point is this summit is all about authentication, but I believe this is probably not going to be the last summit we have, and I would hope not, because the whole issue around accountability comes behind it, and we've just barely scratched the surface on it here. And there's a great deal that we need to do to implement many of the tenants that were in the document that the ESPC issued in terms of Project Lumos, and one of them is to be able to separate out commercial from noncommercial email, be able to signal what class of mail is actually being sent to the ISP so they can differentially treat it, which they haven't for the most part until now.

And so many of the reputation system developers are beginning to think along those lines now, recognizing that regardless of how one might view reputation, the transactional email, the type that you're sending out, which many of our clients do, too, are legally obligated notices, needs to be treated very differently.

But, so I think that recognition is coming. It is not there today, so the relief is not there for you today, nor for our clients who are engaged in transactional email.

To the second point about uneven implementation, on authentication, that's why I strongly believe it's imperative that we have a very simple, easy, singular standard to implement when it comes to an IP-based solution. And then allow the ISPs, now look, I have a strong preference for Sender ID, and I don't pretend to hide it, but let them apply what they believe the right method of interrogating that record is, whether it's the Helo or whether it's the from address, the PRA, the return package, it doesn't matter, but don't ask senders to publish more than one. And that at least gets over the uneven -- or the potential for uneven implementation on the sender side around authentication.

Reputation is a different issue. That's something we should debate further, but I think the general way that we seem to be trending in these solutions is you either establish reputation for the specific mailer, or a line of business if they happen to be a major company, or the ESP that may be sending on their behalf assumes that responsibility on themselves. So that Margaret, for instance, might warrant that this class of small business mailers has a reputation that the ISP should establish.

MS. COLEMAN: Okay, that's a very good question, because we have a lot of panelists who would like to respond. I'll take one more. Fred Lindberg, would you like to respond?

MR. LINDBERG: Yeah, I just wanted to say that what the authentication is on the sender side is really just publishing information. So, you make information available, it's the recipient and the recipient implementation that controls what happens. That's number one.

have clients that really want us to work with this. We have clients for whom the end-to-end or edge model is the preferred one, we have others who said let's just get going.

So, I think the important thing for the senders is to put the information out there, not so much to affect how their messages are judged in the short term, but to give the recipients information so that they can start testing these different models on the recipient side, because it is the recipient end that controls, and the whole point of this is to make it easier for the recipient to control what they receive by basing the authentication on the reputation of the domain of a company or of some type of legal entity, rather than basing it on an IP address.

MS. COLEMAN: Let's have another one from the audience. There's a gentleman there, my far left. Yes, sir? Sorry, Colleen.

MR. BERLIN: Hi, Duane Berlin, B-E-R-L-I-N.

Just a word about thinking ahead a little bit beyond the technological solution that you will arrive at which will ultimately be a tool to identify bad actors. There are several trade associations represented in the panel, there was a question from a trade association of which I'm a member, I'm here on behalf of the trade association. I think it's important for all of us to think about defining what good actors are through the use of self regulation, through the use of the minimum standards that are in the CAN-SPAM act. To the extent that, you know, CAN-SPAM is not applicable, for example, researchers and first responders and other sorts of email that are sent out. Obviously self regulation is necessary there and there needs to be some set of standards for what a good actor is, rather than just I know it when I see it. And coordination between the way those self regulatory and legal standards are implemented, and the way the ISPs ultimately use them to weed out the bad actors.

We certainly applaud the work on behalf of the DMA, they have done a lot in that regard, some of the other organizations have been casual. We have also begun to implement those and some uniformity on that level. Once you have the tools, the technical tools, the real world implementation, which is what this is about, is going to be based upon what is a good actor, as well as what is a bad actor.

MS. COLEMAN: Thank you. John Greco, please.

MR. GRECO: Quickly a comment. I know we're running short on time. Very quickly on that. I think a point that needs to be made is that reinforcement about the separation of good and bad actors. On the bad actor side, a point I was going to make that relates to that, is that technology is one tool that narrows the playing field down so we find out who the bad actors are, and that's why we've been funding the FBI work and closely with them on Operation Slam Spam, and really being able to ferret out the bad actors and therefore prosecute them, convict in some cases, and while we do that, then we sort those out. By having authentication, it really narrows down the playing field of who they're looking for. In the mean time, we continue to work on raising the standards and implementing ethical practices. So, I think it's got to be a multipronged strategy.

MS. COLEMAN: Trevor?

MR. HUGHES: So, I think it speaks to a holistic solution, and the Email Service Provider Coalition -- so, I think it does speak to a holistic solution, and the ESPC has been thinking about this problem in a number of areas for a while. Technology, with authentication and reputation and accreditation, is one of those components. We also see industry best practices as one of those components. We require our members to adhere to what we call the pledge, and it's a consent-based emailing standard. We think those are important, and we think other trade associations should be considering similar type standards, but there's two other components. One is legislation and enforcement, and we have the CAN-SPAM Act now, although the case didn't come under the CAN-SPAM Act, we saw a nine-year prison sentence issued in Virginia just recently for a spammer. I think we need more of those perk blocks. I think we need spammers to see on the 6:00 news the spammer with a raincoat over his head being ushered out of the courthouse and off to jail.

We joked about it during the CAN-SPAM run-up before it was passed that, you know, as a trade association, we were okay with the death penalty for spamming, and that may sound paradoxical, but, you know, indeed, we actually are very supportive of strong deterrent facts or effects in this space.

The one component that I think is missing that I have not heard a lot of discussion about yet, is consumer education. And I think we as an industry are failing in that regard so far. In fact, we're failing pretty miserably. Consumers do not know what they do with their email address that exposes them to spam.

CDT did a great study last year that shows that consumers that post their email address on a chat -- in a chat room, on a public website, in a news group, that those are getting scraped and it's generating spam.

Consumers that give away their email address, here's a big surprise, to a gambling or pornography website, gets spam. I don't think consumers generally are making those connections, though, and I think that's one big area where we haven't -- we haven't done enough work yet.

MS. COLEMAN: Okay, and so it's 12:05, I apologize, but it looks like we're going to have to cut this a little short, but I encourage you to visit with our very good panelists and raise your questions, but for now, enjoy your lunch, and I hope to see you when we return. Thank you.

(Applause.)

(Whereupon, at 12:04 p.m., a lunch recess was taken.)

Schwartzman from Canada, and unfortunately, Neil had a last-minute conflict and is unable to join us, but John Levine has graciously agreed to step in, and I'm told that John does work closely with Neil and with the Canadians on their fight against spam, and in fact John tells me that he makes his own maple syrup. So, that makes him very qualified to play a Canadian on TV here today.

Now, we also have a fourth panelist and I'm pleased to introduce John Levine. And we've heard from John before, and John has been writing and consulting on email and the Internet for over a decade. And perhaps some of you even have his book on your bookshelves, Internet for Dummies.

Now, this panel is going to focus on the international issues relating to authentication, and when we first organized this workshop, we were thinking, you know, what's the best way to focus on the international issues, because really, isn't authentication by definition an international issue? Isn't the Internet an international medium, and hasn't email allowed us to communicate with our friends and family and business colleagues all over the globe?

So, by definition, authentication is an international issue, and we actually have heard some of the concerns that we hope to explore a little bit more this afternoon. We heard about them earlier, and I just want to highlight a few of them, with the hopes that our panelists will address them, and if they don't address them, we will be certain to make them do so during the question and answer period.

One issue is do we need compatibility and harmonization across the globe for authentication to actually work? We actually have heard some conflicting things. Some people are saying that these different approaches can co-exist, and other people are saying that we need one approach to make things seamless. So, if our panelists could address that issue, that would enlighten us a great deal.

A second issue that was raised, and it was early on in the conference, and I think it was one of the most important issues, at least for consumers, and something that the Federal Trade Commission holds dearly, and that is free speech. Now, in the United States, we have the First Amendment, but in other countries where the First Amendment doesn't apply, how are we going to deal with that issue? Do we want authentication to prevent asyor consumers, and sometnvs15   kf3em   20   First At6p to

Dave Crocker, who has a PowerPoint and I will ask him to step up there.

MR. CROCKER: Thank you, Yael, I think. But with -- I don't have any prepared humor, so I'm not quite sure what's going to happen now that she set you up that way. It's a little strange being an American being asked to talk about international issues, and so I should explain a little bit about where my perspective comes from.

On the one hand, having worked in the Internet for a long time, and having the Internet have a really rich array of international participation, the different character sets.

More personally, I was the accompanying spouse when my wife had a one-year fellowship and we lived in Malaysia, and unbeknownst to Yael, I actually lived in and obtained landed immigrant status in Canada. And the most interesting thing to me about that relative to this group is that over the course of the year I was living there, I kept coming into the U.S. and chatting with people and, you know, they said, "how do you like it?"

the instant you have an operation that's actually trying to coordinate on problem solving is really when this gets quite serious. I've had some ongoing discussions with the branch of the Chinese government which is officially a trade association, except that all of the members of the board are part of the Chinese government, that work on behalf of Chinese ISPs, and China has had the distinction of being assessed as the primary source of spam-sending engines in the world. And last spring they decided to do something about that.

So, there's been some ongoing discussions, and within four months they moved into number two, which may sound pretty terrible, and it is, but that represents real change, and it came about because they focused on it when they hadn't been before. And there's a long way to go, but it shows that when there is a desire and effort to make some international cooperation, there can be real progress.

The other aspect of working together is that the rules of etiquette are so vastly different. And the other two comments I wanted to make are a little bit about technology and a little bit about operations. So, on the human factors, we know that different countries have very different privacy rules. Yael commented on that. They have very different rules about

which I mean the people who really are responsible, but they might be more aggressive than some of us would like.

The other folks, the folks who are hardcore spammers, I'm increasingly comfortable with the tendency to call them criminals, because I'm not a lawyer, so I get to dandy that term around a little more loosely than some, and I think it gets at the psychology, the aggressiveness and the cleverness far better than just different ways, therefore they don't match on a string matching basis, but they look to the recipient very similar. And so nonbreaking space versus space and so on and so forth.

And in general, when we talk about canaliculization of the data in order to assess whether it's the same, whether it's -- or whether it's been transformed in a meaningful way, each of these encoding differences can make things quite a bit more challenging, and I have mixed reactions about whether I'm happy or sad that John pointed out unicode opens the door further, but we do need to make sure our protocols support that.

It's really a very distorting reality to experience high quality Internet access all the time, because it makes you think, well, that's where everybody's going, and that might be where everybody's going, but going means future and future for the Internet is measured in five and ten-year increments for these kinds of what are really paradigm shifts.

Much of the world has truly terrible access. It's dial-up and it's very slow, Indonesia this summer I was considering it really good to get 19-2 access and it was expensive. And so when we start assuming that people will be able to make cross-net queries, we need to be a little bit judicious about that. The difference between one cross-net query between MTAs and ten cross-net queries between users is probably the difference between working and not working.

And then lastly on operations, I emphasize the issue of establishing trust, because I think that the single most important international issue is to get communications between operations groups. There are informal versions of that on the net today, and they work remarkably well. No, they don't work remarkably well, they work exactly as well as you would expect them to because the people are motivated. But there needs to be more of that, and it needs to be -- it needs to be operated in a way where the trust is real, and I think, by the way, that's something where governments can help enormously.

I don't believe that the communication can be -- the realtime communication should be between the governments, but I think the governments can facilitate the exchange. And a simple example of that would be services for realtime language translation, used by the operators. And I can't remember whether it was a Chinese ISP or a Korean or Japanese ISP that came up with that idea of having online translation services for the operators.

Thank you.

(Applause.)

MS. WEINMAN: Thanks, Dave, you raised a number of issues, and I'm hoping that we can address some of them further in the discussion period.

Now we'll hear from Hadmut Danisch.

MR. DANISCH: Okay, thank you very much for inviting me. I am the international part of the international panel. And I am supposed to say something about international aspects, and one of these international aspects of spam just struck me on the way to the lunch, when I just went to lunch to the Union Station, there was a nice looking girl and she gave me something, here, take that, and I have to admit, I was looking at the girl and not at what she gave me, so I took it, and it turned out to be a brochure of Canada asking me to come to Toronto. So, also a kind of international spam. Yeah. So, it's actually a pity that Neil Schwartzman from Canada isn't here.

MS. WEINMAN: We can pass it on to John Levine who is pretending to be Canadian today.

MR. LEVINE: I'll take it back up.

MR. DANISCH: Today I would like to do two things. The first thing I would like to do is to disappoint you. The second thing is I would like to come up with a new proposal, freshly made, especially for this summit. It's so fresh that it doesn't even have a name yet.

Let's start with the bad news. Authentication, and that's what this summit is about, is just the first step. As Harry Katz pointed out yesterday, authentication means forcing the spammer to come out of his cave and say, "here I am, shoot me." But that's pointless, as long as we don't have an international weapon. If one doesn't have a gun, there is no danger in coming out and saying, "hey, shoot me, shoot me."

So, what we need to do is have a second step, about liability or accountability, and this second step must include an element of authentication. So, authentication is not pointless, it is important, but it's just the first of two steps.

And that's actually the problem, because we have to solve this problem on a worldwide scale, and that's what I'm going to talk about. I will start today that spam is a global problem, and we do need a global solution. And my point of view is there is no global solution. That's the bad news.

There are about 250 countries, and every one of these countries has a different legislation, different mentality, and different ideas of privacy and a

addresses to countries. So, I've sorted the spam by the country of the IP address of the sender. So, it has not yet to do anything with the domain or the sender address, it's just the IP address.

And the result was that about a quarter of the spam comes from the United States, another quarter from Korea, a third quarter from China and the fourth quarter from more than 100 countries around the world. What does that mean? Not too much, actually. Because it might look completely different once a domain authentication scheme is in place, and the domains might look very different, but it gives a very good method to have a first reality check. Whatever you do, whatever you propose, whatever technical measures you find, ask yourself four questions. The first question is, does it work in the United States? The second question, does it work in Korea? The third question, does it work in China? And the fourth question, does it work in the 247 other countries of the world? And I believe that's a very tough, very hard question, very difficult to answer.

So, what I would like to propose is to solve the problem in a different way. I propose to block all emails coming from generic top-level domains, such as .com, .gov, and all the other top-level domains, and to use only country code top-level domains for sending

And things like that must obviously also not be allowed under country code top-level domains to work.

So, what would be the result of this? Every country would have its own job to keep its own country code top-level domain clean, and this allows every country to find a solution suitable for its own needs. So, there are currently about 250 countries and the number is not significantly growing. In contrast to domains, it is not yet today this domain, tomorrow another domain and there are no disposals of the countries known yet. Yet, maybe next week.

So, it is up to the receiver to -- the recipient's MTA administrator to build a table of these 250 countries and how to treat mail from every country differently. For example, I receive very little spam from the northern part of Europe, Finland, Sweden, Norway, and I would just open my mailbox for them without any further check.

On the other hand, I never received anything useful from Korea, so I would completely block them, and I receive most useful mails and spams from the United States, so I would drive all those mails from the very top, about 20 mail spam filters. And it's up to everyone how to configure their mail system and how to treat the different countries. And this is all the key to fight phishing, because once you know which country a mail comes from, it's very easy to configure your mail reader to display the country and it can say, yes, this is a country coming from America, and throw the flag and play the anthem and everything you need. And this way you can even tell your 74-year-old grandmother, or people not experienced with Internet, to not trust anything which doesn't come from the United States, because if they receive an email telling you this is your -- this is about your bank account, and the sender address in Korea, everyone wakes up and says, "oh, there must be something wrong." And even if they don't understand the Internet game, just tell them it's patriotic, don't trust anything which doesn't come from the United States the source of these.

So, even those people who are not experienced with Internet have at least a simple way to tell us this email comes from my own country, or from a different country, and if it comes from my own country, and still is phishing, you have a chance to prosecute, because those domains must be given only to people awaiting prosecution. That's it.

(Applause.)

some of the more tech-oriented people in the audience, and we know we have them here, because they spoke earlier in this summit, might have some reaction to this proposal and some questions for Hadmut.

Now we're going to hear from John Levine, who is going to inform us about what's happening in Canada and other goodies. Thanks, John.

MR. LEVINE: And other stuff. Thank you. I didn't realize that I had an actual Canadian on the panel here with me, and I understand the situation in Canada reasonably well, but I can't do the accent, ey, so you'll just have to bear with me.

But Industry Canada has had a task force going for about a year on spam in general, and they invited me fairly early on to be part of it. And I live far enough north in New York that Toronto is actually the closest big city to me, so I'm up there all the time anyway, and I go up and I chat with them. And I discovered a couple of interesting things, and like Dave said, although Canada looks like the U.S. if you're not looking too closely, there are a variety of ways in which it's quite different.

Their Internet industry is quite different because they only have, unlike the U.S. that has a vast number of ISPs, they actually have three and a half big

ISPs and a thousand little ones. The big ISPs are Bell Canada, which is the phone company in eastern Canada, Telex which is the phone company in western Canada, Rogers, which is the cable company everywhere, and Videotron, which is the cable company in Quebec.

And those then comprise the vast majority of the Canadian Internet infrastructure, except that they also have about a thousand little mom-and-pop ISPs, and small Canadian businesses, of which there are many, tend to use the small ISPs.

So, we heard this morning a fairly eloquent comment that whatever we do has to work for little businesses here in the U.S., and that's equally important in Canada and in other countries.

As far as what Canada is actually doing, they're doing -- a bunch of the stuff is specific to Canada that are not too relevant here. They're always concerned with what specifically Canadian issues are there and there are all sorts of issues, bilingualism, and anything that only happens in English is flatly illegal in Canada. But they can deal with those.

And what they have been working on are two things that actually start to get around towards the issue of authentication, they've been working on related efforts and best practices and certification. And these are best practices, particularly for bulk mailers.

Canada has a moderate number of bulk mailers, they have far fewer spammers than we do. I mean, I can only think of one really serious spam center in Canada. And they have a -- and they have a remarkably enlightened direct marketing industry, and in particular the Canadian Direct Marketing Association, unlike the American one, has long agreed that it's not -- it's not in the marketer's interest to send email to people who haven't asked for it. They concur with pretty much everybody else that bulk mailers should only send mail to people who affirmatively opted in.

Furthermore, Canada has a privacy law called PIPED ACT, which is about this thick, and most Canadians -- I have not met any Canadians that purport to understand it in detail, and I certainly don't. But it's similar to European privacy laws about under what circumstances can you collect data, and under what circumstances can you transfer them to other people. And that both affects mailers and it also ties into best practices and certification and reputation systems, because of course you know a reputation system that -- you know, a reputation system is like a credit bureau. And a credit bureau is sort of by design a privacy disaster. It's a, you know, it's a bunch of -- it's a bunch of information about you kept by people who by and large have interests opposed to yours. And you want to make sure that if they lend you money, you'll pay it, you know, and otherwise they -- if you've done something bad, they want to know about it.

So, the Canadians have been talking about best practices and they're actually making some progress towards coming up with a best practices code for Canadian mailers and we're going to have yet more meetings about it. And they're talking about certification. And that is an area where actually, although authentication, the technical aspects of authentication have to be the same everywhere.

And they asked at one point, is there anything special we should be doing here in Canada? And all the tech people on that group said, "no, of course not, but what you need to do is make sure that whatever you do harmonizes with the U.S. and the Bureau."

But the issue of reputation, I think actually sort of related to what Hadmut was talking about. Canadian mailers are mostly mailing to Canadians and American mailers are mostly mailing to Americans. And the sorts of reputation systems that you're going to have for bulk mailers really are largely country specific.

It would not be particularly productive for me in the U.S. to try to collect reputation information about Canadian bulk mailers, because even the bad ones don't mail to me. And vice versa. You know, somebody in Europe wouldn't collect too much -- wouldn't be able to collect much useful information on legitimate bulk mailers or mainstream bulk mailers in the U.S., because they don't mail out to Europe.

So, as far as both the certification of good practice and reputation stuff, that's actually a place where country-specific activity is necessary. And I think we're going to see American reputation services here, Canadian reputation services in Canada, and in Europe, I don't know whether they will be EU specific or country specific, but they will certainly be geographic specific.

So, that's what's happening in Canada. I think in some ways they're a little farther ahead than here, just because the country is smaller and a little less heterogenous and they're somewhat less of the wild west approach to Internet business practice.

Now putting on my other hat, turning back into myself, I went to the International Telecommunications Union World Symposium and Internet Society Preparatory Meeting to the Tunis Phase of the WSIS Process Special

Meeting on Spam. I believe that's what it was called.

MS. WEINMAN: Could you say that again?

MR. LEVINE: No. It was the ITWSIS spam meeting. But it was the meeting, it was in Geneva, at the ITU, which is across the street from the Geneva part of the United Nations. And a nice thing about having it in Geneva is that every country in the world has a permanent representative of some sorteE740Ed has a can compete on a level basis with those big rich Americans and Europeans. That's what they used to say.

Now, at this meeting, what they are saying is spam is awful, spam is killing us. The representative from Syria, who apparently is noted for his eloquent speech at these sorts of meetings, discussed with considerable vigor at some length, and you know what that means, the effect that spam has on them. And he said that the first and most direct effect is that it costs them vast amounts of money. I mean, small countries tend to be at the end of long, thin, expensive Internet connections. I mean, if you're trying to get an Internet connection into central Africa, really your only alternative is a satellite connection, and satellite connections you pay by the bit. So, as the spam comes in, the meter is running. So, for them, you know, the Internet is too dangerous and too crooked for us even to deal with. And that is, you know, potentially really sad. Because I heard stories about countries, again, specifically in Africa, because that's where this woman was familiar with the situation, but these are countries that were basically drawn on the map by English Imperialists 150 years ago, and they are random collections of mountains and swamps that have never had any sort of national identity. And even though these satellite connections are expensive, they exist. And the Internet gives them the possibility of actually having offices in rural towns and have their firstections are expensivdtime expensive,000jck. Aheir

One is merely the issue of, all right, we've tracked this spam down and it's coming through Cameroon. Is there a Cameroon ministry of telecommunications? No. Is there anybody there who knows anything about the Internet? You know, maybe, maybe not. It's not because these people are stupid and ignorant, it's because they're poor. You know, if you make a list of major national urgent points, you know, somebody who knows about spam may not be too high on the list.

these countries, I mean they all have some sort of legal code, but it's not necessarily like ours, but being able -- the more specifically you can know, this is who we're after, this is the kind of information we're looking for, that makes it much more -- much more likely that if you need to go to another country that you will be able to ask them questions that they're allowed to answer.

I mean, in Europe and in Canada, we have privacy laws, so you can't just go on fishing expeditions, because you think somebody might have done something bad, you need a reasonable legal case, and authentication really will help us do that.

So, it's all kind of a piece. You know, and this has nothing to do with whether it's Sender ID or Domainkeys or anything like that, but it has everything to do with being able to say, we got this piece of mail, and we have evidence that will stand up in any sort of regional court that it was sent by this organization through this point. So, I think this is the kind of stuff that we need to work with countries all over the world, but particularly the less developed ones.

So, that's both sides of my brain now.

MS. WEINMAN: Thank you, John. We actually know more than one person in Australia. So --

MR. LEVINE: Well, actually, the chair of that meeting was from Australia, and he was extremely effective. Australia clearly has their act together.

MS. WEINMAN: Just because we are in an FTC building, and John mentioned the MOU, I would also like to mention that at a recent meeting in London, it was a meeting that gathered all these spam enforcers around the globe, and an action plan was developed and Commissioner Leibowitz spoke about it a bit this morning, and these are countries that have come together to work together on enforcing spam. Now, they recognize that the laws are different in different jurisdictions, and that's -- that's just a reality, our laws are different in many other aspects of life.

So, and I encourage you to look on the FTC website, and if anyone wants to approach me at the end there's somebody here from Korea." So, we want to hear from you, and we also want to hear from the rest of you.

So, please raise your hands with any comments or questions you might have. And the roving microphone folks will be roving.

MR. SCHNELL: Ron Schnell, Equifax. Hadmut, how do you propose authenticating the top-level domain, and what do you suggest we do with Tuvalu or do you want to just consider that a generic domain?

MS. WEINMAN: Can you repeat the second part of the Tuvalu, what is that?

MR. SCHNELL: The great island nation of Tuvalu, TV.

MS. WEINMAN: .TV, okay.

MR. CROCKER: And I'm going to guess that the point is that there are some national domains that are operated in ways that look an awful lot like generic domains.

MR. DANISCH: Authentication is all -- once you have the domain part, indicating the country code top-level domain, you can even have authentication specific to any country. There's another problem. Yesterday we heard a lot about cryptography and using cryptographic methods for authentication. There's another problem, because once you have a system for email authentication, it can very easily be turned into a property encryption scheme because you just need to add a country IP exchange and I'm quite sure that many, many countries won't allow this.

If I were a country without democracy, a government of an underdeveloped country, I would never allow cryptographic mail authentication, even worse, if

illegal to have reputation of an individual in many countries, but reputation of an address was not necessarily a problem.

And that there was, also, a strong undercurrent of kind of enforcement and, you know, all we need to do is stop this stuff at the source, and I don't know about you guys, but I think most of us have pretty much given up that stopping at the source is not going to work. You know, I need to be able to stop it where I receive it, not where it's sent.

So, I would just suggest when we think about many of the other countries of the world, we've got to understand their view of this problem is just not as progressed as ours, because frankly their environment isn't nearly as nasty. But it probably will be fairly shortly.

MS. WEINMAN: Okay, we probably just have time left for our two panelists to respond. So, Dave?

MR. CROCKER: The comment about stopping at the source strikes me as an important one. I haven't given up yet. I don't think that we can stop all spam at the source, but one of the major benefits of being able to hold operators accountable is that as an operator is identified as being a spam friendly haven, such as $10,000 will get you any webpage you want, was the example that John Levine had, then there will be incentives for those operators to clean up their act.

This won't eliminate spam, and one of the international aspects is that as we find one country tightening things up, the spammers move to another. The estimates I've heard from some is that the next hot spot will be Russia. And that's just because their laws will be a little bit looser, and if that tightens up, they'll find another place. And as Hadmut points out, there's a lot of countries to choose from.

MR. DANISCH: Getting agreement of so many other countries would be very hard. For example, in Europe, finding an agreement in Europe, you will have a very hard time. So, that's another one of my proposals, if you start to ensure trust in U.S. domains instead of trying to secure the whole world in a first step, then you have something which is completely under U.S. control.

You have to -- you don't have to ask anyone else for agreement, you can do whatever you think is best and can start with it and say, okay, we have cleaned up our own domain, it worked, here is proof, all other countries, please follow us if you want to participate in the worldwide email system.

So, this would be a good point to start for an experiment and to demonstrate how it works, because you are currently at the very lucky position, you are the only country which is that far in fighting against spam. So, it would be very nice if United States gave a good example and started with one U.S. domain as an experiment.

MR. CROCKER: I wanted to toss in one more observation, as we think about the diversity internationally, it's also sometimes good to think about the similarities. John made a comment, and I don't get to pick on him very often, so this one is kind of fun. He talked about the privacy laws that we have here in the U.S. and in Europe, although my sense is frequently the Europeans don't think we have much privacy law here in the U.S.

What was fascinating to me -- what was fascinating to me at the first workshop that the Chinese held in Beijing, sitting up on a panel with a collection of government and ISP kinds of people, and I grew up during the Cold War, I have what is, I think, a pretty predictable set of training and expectations about what mainland China was and therefore presumably is about, and it was so completely wrong, it was devastating.

I found myself when I legs400000h5rom that0000 0.00000 0.0

in trying to think about how to interact and what was possible was more like western Europe.

One of these panels included policy makers and government officials and ISP folks, and there was a very explicit focus on discussions about privacy. And point for point, word for word, emotion for emotion, intensity, seriousness, earnestness and all the rest, it matched every other panel like that I've ever seen in the U.S. And this was in China.

MS. WEINMAN: Well, thank you to our three or four panelists, and thanks to the audience for some interesting questions and comments.

(Applause.)

MR. SALSBURG: We'll be starting the next panel in 30 seconds, so it's not break time yet.

Good afternoon. In this panel, we're going to talk about kind of a culmination of where we've been so far. We started yesterday looking at some of the policy issues talking about main level authentication, whether it be the IP issues, or antitrust issues, privacy issues. We moved then to hearing what several of the proposals are. We've heard some analysis of those proposals, and we've seen how spammers might try to circumvent them. We've heard some of the international issues that are involved, and some of the practical issues that are also involved. And now, this is actually our last panel that's going to deal with authentication. Because the final panel, before the closing remarks, is going to deal with what comes after authentication.

So, what do you do in a final panel that deals with authentication at the authentication summit? Well, I think what you do is two things. One is you try to bring together the proponents of all the different authentication standards, and figure out, first, what are those remaining issues that need to be resolved, and second, how do you get these authentication standards out into the community and get them tested and implemented and get them implemented quickly.

So, we're actually going to do something a little bit different in this panel than we've done before. But I'll save that for a surprise and I'll first introduce who the panelists are.

Down at my far right, is Brad Garlinghouse, he's the Vice President of Yahoo!, and he is here to talk about DomainKeys. Next to Brad is Jim Fenton, from Cisco to talk about -- did I go in the wrong direction? Somebody moved the cards on me. Jim Fenton is over here to talk about Identified Internet Mail, he's from Cisco. Dave Crocker is right next to me, and Dave is here to talk about BATV. For Sender ID. There's Ryan Hamlin, Ryan is right there, and next to me, Meng Weng Wong, who is the author of the SPF protocol, which has been incorporated into Sender ID. And Doug Otis is right over here to talk about CSV.

So, here's the surprise: In all the panels that we've done so far, what we've done is saved Q&A for the very end. Here we're actually going to do it in reverse. And the reason is this: The technological sophistication of the audience is pretty high here, and if there are issues that go to any of the particular standards, if there are glitches that you would like to have the proponents of the standards address, if there are things that you think should be included in the testing machines as they're designed, here is your chance to speak up and hear some responses.

So, with that, we are going to move to a little bit of a town house style panel -- town house? Town hall. Town hall. Right. A condominium type of panel. So, we have the roving microphones, and why don't we begin by taking the path-based or IP-based domain level authentication proposals, and throwing out to you out there, do you have any questions for the proponents of these proposals about how they might affect certain types of email transmission, or things that they might want to look for when they're testing?

Why don't we start with this gentleman right here who raised his hand. And if you can identify your name.

MR. HANSON: Tony Hansen, H-A-N-S-E-N. Both the SPF and the Sender ID have problems with forwarded mail. SPF doesn't handle it at all it seems and Sender ID requires modifications to the way we handle forwarded mail, requiring additional letters to be added when mail is forwarded. I was wondering if those two proponents could address that issue a little bit.

MR. SALSBURG: Ryan or Meng?

MR. HAMLIN: I'll start. So, kind of one of the observations I've had over the last, it's been 48 hours, is that there's been a lot of good proposals that have vented a lot of the issues for the most part have been raised. This issue with forwarding with Sender ID/SPF certainly is a known one that we've talked about. I know in the IETF many, many times. And what we tried to do with Sender ID obviously is acknowledge that, yes, there are certainly some issues, and we've proposed, I know in the spec, ways to get around those. But, you know, from my perspective, is the best way to continue to vent these out is to test them, and that's kind of the call to action that we've been talking about for the last -- I guess the last two days.

And so, specifically while forwarding we need to know all those scenarios. I think we know a ton of those today. And we have examples out there today that if it's this particular forwarding situation, you have to do this. If it's this kind, you have to do this. We probably have missed a few, and the way you find those is you test in real life.

That's why, I mean, we wanted to be very clear coming here is having that call to action to say we need to -- let's find those remaining cases that are out there. We think we've nailed the majority of them and like I said, they are defined in the spec with use cases, and Harry walked through some of those yesterday, and that's, you know, that's our response to this is we're going to continue to find those fringe cases, and when we do, we just need to work through them. And that's kind of our call to action today is let's move forward and start to implement those.

MR. SALSBURG: And Meng, do you have anything to add to that?

MR. WONG: Yeah, I do. First I would like to address the little misconception there that SPF does not have an answer to the forwarding problem. We do have an answer, it's called SRS, and it sucks. So, it's really --

whitelisting. Like I got mail the other day from eBay, and it happened not to be forwarded to me, it came straight to my address, and I was wondering whether it was from eBay, right, and so I looked at the SPF result, because eBay is now publishing its SPF records, and it says, yes, this really is from eBay. So, that's an immediate win that SPF gives you, even if forwarding is a problem.

But I think the final answer is none of these solutions are really a final complete solution. And for a solution that doesn't have the forwarding problem, we need to look to crypto. We need to look to solutions like DomainKeys and IIM and things like that. And so, one day, I hope, everybody will be using crypto, and when their mail gets forwarded, we will be able to look at the crypto result and say, it passes. So, I'm looking forward to that.

MR. SALSBURG: There's a hand raised in the back there, Sana.

AUDIENCE MEMBER: William Wu [phonetic] from -- (inaudible). There has been a lot of information that for Sender ID, which consists of now two parts, SPF and PRA, that PRA is going to be used in mail user agents, and SPF is going to be used in MTAs. Now, the MUAs are basically final programs that they got the mail from the

ISPs, they are not actually involved in the mail delivery. So, I'm concerned that the IP-based authentication technology is going to be used after -- after the fact -- after the delivery already happened.

And in this case, you're going to have to rely on the security data about what kind of a -- what kind of MTA transaction took place. So, I'm concerned that in this case, it's very difficult to have PRA work with mail user agents and if it's the case that PRA is being promoted for the final mail user agent, it's not going to work very well.

MR. HAMLIN: Meng, I know you wrote some stuff in your white paper about that, but I'll start. One clarification that I have actually been hearing, this is a quick side note, the Sender ID framework includes, just so everyone knows, when we talk about Sender ID, there's been a lot of discussion with (inaudible) I publish my SPF record, but I also publish my Sender ID record. And technically there is one framework that's called the Sender ID framework, and within that framework, there's one way to publish a record, it's actually the SPF record.

So, we've always been very clear, you publish your SPF record. Within the Sender ID framework, you have multiple ways of checking that, right, so you can use the mail from, or you can use the PRA check. So, I just wanted to make sure we clarify that. There's been a lot of I think confusion over the last couple of days when people say SPF and Sender ID. Sender ID is a framework.

But to your question, I can speak on how Microsoft is going to implement it. It's hard for me to speak on how others will do that. It's a choice, again. I know Meng has said that PRA would be at the MUA level and the mail from would be at that MTA. In the case of Microsoft, I know at Hotmail we will be checking the PRA and we will be doing that at the MTA level. Within Exchange we will be doing that at the MTA level as well. Certainly we will pass that parameter down to our clients, in the case of Outlook, so they can actually have that as well.

So, it is a choice of how you want to do it, and that's how Microsoft is moving to do it, but others will have to decide where they want to make that check.

Meng, do you want to add to that?

MR. WONG: I will add to that. I think in sort of integrated situations like Hotmail, it's very hard to distinguish exactly what is the MTA and what is the MUA, because the whole thing is one monolistic stream.

MR. SALSBURG: The gentleman in the front row here, Colleen.

DR. HALLAM-BAKER: Philip Hallam-Baker.

Since Sender ID is a framework and in the aims of or the objective of greater harmony, would it make sense to add CSV into the Sender ID framework as well? The question really is to Ryan, are you prepared to add the helo checking, and to the CSV people, are you really, really going to insist that you have your own DNS record to publish? Will you make this change or do I have to write the RFC?

MR. SALSBURG: Ryan, do you want to go first and then we'll turn to Doug?

MR. HAMLIN: So, you know, we've spent, as you know, Phil, we've spent a ton of time, I remember sitting at this exact table 18 months ago proposing this little idea we had called publishing IP addresses in a text record and solving the problem. So, while I'm all for, certainly, you know, taking the very best of what the industry has, we need to do that. There's a point in time where you have to basically say enough is enough and we have to move forward and we have to start testing these things out.

Now, if it turns out that the CSV stuff could be put in and it's seamless and it works, we can move just as quickly as we are now. Certainly, I mean, I think any objective person would say, "yeah, that's fine," but we have to look at that and say, "is this going to slow us down?" You know, we already have 180,000 domains that have published SPF records. I just talked to the Hotmail guys and got some recent data yesterday. We have been monitoring how many people are actually publishing SPF.

So, roughly 12 percent of all the domains that come now to Hotmail are publishing SPF. Of that 12 percent, though, the interesting stat is that that represents about 35 to 40 percent of the mail. In Hotmail, you know, we get about three to four billion messages a day. So, we already have -- this is moving along. The train left the station. So, we have to make a very conscious decision, do we turn the train around and add to it or do we continue to go forward and ship our V-1. I mean, I've been shipping product at Microsoft for ten years. There's a lot of important value in a V-1 shipment. And then you listen to your customers and you go back with a V-2 and you grab those best of features and put them in V-2.

What I would like to see happen is that we continue with the train going forward with our V-1 release.

MR. SALSBURG: Doug, has the train left the station or is there time to get your caboose on?

MR. OTIS: Well, to clarify a bit, when you're talking about the whole domain, you're not talking about a mailbox domain and that those are two different labels and they're going to result from two different records anyway.

The CSV record is very efficient, it gives back specifically that host and you don't have to run through a script hosting engine to decide after 100 or so queries, yes, this is the host that I should be talking to.

So, in that respect, I would hope that if we are going to implement CSV, it won't be using this thing that has a great deal of legacy of running through trying to effectively query the world to decide have I covered all the bases for all the possible hosts that might possibly send that mailbox domain. It's just overwhelming for DNS and it's -- CSV is designed to be very lightweight, to be very efficient, and effectively get everything done in one shot. That's not been the design goal for either SPF or Sender ID. That, you know, those two different design goals are why I have such resistance to suggesting that SPF somehow incorporate more of the world, and that we have already a great deal of anxiety, gee, when I publish SPF, am I talking about qualifying my mailbox domain, am I qualifying my PRA, am I qualifying my helo domain now? You just don't know when you publish that record what it is you're applying it to.

I think it's best done, because it's already a different label anyway, it's best done with a label specifically for that task. I mean a record typed specifically for that task.

MR. CROCKER: There was actually quite extensive discussion on the MARID mailing list, back when there was a MARID, about exactly this question of having CSV use SPF records. There seemed to be a pretty strong consensus not to do that, which makes me really interested to see what Carl Hutzler's experience turns into.

But the bottom line is that an SPF record is trying to publish one kind of semantics, and CSV thinks it's looking for another. So, if there's a way to re-use the original semantics of the SPF record, that would be interesting, but kind of surprising.

A very different issue is, we want to be careful about trying to push everything under one umbrella when it's actually a variety of different mechanisms. Because that would give an appearance of homogeneity, when that isn't the fact.

MR. SALSBURG: Sana, this gentleman in the front.

rest that's out there, but leaving the rest for the later technologies, like BATV, CSV, DomainKeys, IIM, as better solutions for those pieces.

Is that a reasonable approach, or are there problems with moving ahead with that? Thanks.

MR. SALSBURG: Let me begin by saying that one of the important responses to that question is your own, at AOL.

MR. HUTZLER: Bring that mic back.

MR. SALSBURG: So, I would be interested in seeing the mic go back to you and give us your answer.

MR. HUTZLER: That's completely unfair.

We don't know. You know, I have my own thinking. I have an engineering background, electrical engineer, and there's always trade-offs with design, and one of the trade-offs we've always been talking about, and that is should you do something that's quick, you know, where senders all they have to do is change the DNS record, which is easy and it's quick and it's sort of painless, or do you go with -- or do you throw that off to the side because it's not as good as it could be, and you look at some of the approaches that are better, which we know that content signing solutions, everybody up here, including the IP-based proponents, are, you know, realize that those are better approaches. You know, do we go, you know, do we wait? Is there a danger in moving forward with something that's good enough for some cases, knowing that we need more later? I don't know how else to put it. I don't know the answer.

MR. SALSBURG: Doug?

MR. OTIS: With regard to moving forward, we know that we want to head towards a cryptographic scheme. I think it seems that everyone has that vision as to where we're headed. What we need to get there, I think, is to follow on with that is a reputation system. And I think we've all agreed we need a reputation system.

The aspect that I look at is, can I really trust the identity to give them a reputation. In other words, and can I damage the reputation, because that's what I'm going to do. And I can't depend on something that is not authenticated. And in my view, SPF and Sender ID, all they're doing is authorizing the SMTP agent to send mail that they've never authenticated, because the path leading to them, there's no certainty even what checks have been made on that mail message heading towards us as to whether or not they were consistent on checking the same headers.

We don't know if it's one-hop mail. You're looking at the message and you can't really trust any content in that message to be valid, and so you're left with effectively nothing that you can use as in a name to base their reputation.

And so we need something that we can directly authenticate, and that's where the helo domain came in, because that is something that we can authenticate, and that gives us a starting point for establishing a reputation system.

Karl Jacobs from BlueCall said, well, we will -- Cloudmark, I'm sorry, that was not intended -- said that, you know, "we accept the message and we checked that identity, but we don't trust it well enough to stop there. We're going to run other filters on it." And that tells you, already, that that information isn't really trustworthy.

MR. SALSBURG: Brad, let me turn to you. You've had your tent up.

MR. GARLINGHOUSE: So, actually, first of all, this is the first time I've spoken at this event, I appreciate the FTC and NIST certainly sponsoring this.

The first thing that I have listened to, as sort of a relatively newcomer to these Alpine ski events as described this morning, I feel like there's some great fallacy that we're dealing with and, you know, Carl concluded his question by saying, I think the last word was, "or do we wait?" And I listen to that and I hear that and I say, well, wait a minute, what does that mean? And I know Miles Libby from Yahoo! spoke yesterday about the things we're doing with DomainKeys, and Yahoo! is now virtually signing 100 percent of our outbound mail with DomainKeys, within weeks we'll be verifying 100 percent of our inbound mail.

And when we say Yahoo!, we're also talking about SBC, a very large ISP, we're also talking about British Telecom, a very large ISP, we're also talking about Rogers up in Canada, a very large ISP, and so I think do we wait, do we wait for a couple of weeks? You know, we're talking about -- I very much agree with something Ryan said earlier, also. So, there is a train, and the train is called, you know, Sender ID/SPF, and it has built momentum. By no means am I trying to sit here and suggest that we should turn the train around. On the contrary. We also shouldn't pretend that there's only one train.

And when I sit up here and I hear, "hey, let's wait." I don't know what people mean when we talk about that. Because crypto solutions are not out here in the ether, you know, conceptual. This is real. Q-mail has implementation, Sendmail has implementation, CERN has built a Microsoft Exchange-based implementation. You know, you have one of the largest ISPs in India already doing this. It's not something that's kind of out there, it's here and now.

If we believe -- my big fear, let me get a name here, because Brian Cunningham actually described this morning, and I don't know Brian, but he described this morning an interesting analogy. RMX back in '96, '97 failed. So why did it fail? Well, one of the reasons is it had too many cases where it broke and because it wasn't reliable enough, the train of RMX went down the tracks and then at some point it gained more momentum, but then it's like wait a minute, this isn't the solution.

And so what I fear is if we have to acknowledge there's two trains and we should test both of them and we should try to build increased momentum for both of them. But we shouldn't say there's one train and we'll figure out that other train later on.

MR. WONG: These train problems always have two trains, right?

MR. HAMLIN: Which one is moving further apart more quickly.

MR. SALSBURG: Ryan?

MR. HAMLIN: Just to kind of follow on what Carl said and then Brad's comments. I think it comes down to the choice of the implementer. So, like Brad is saying, they're doing some things, they're moving forward with DomainKeys, signing their mail, you know, on the Hotmail side, we're going to be checking for the presence of the Sender ID records and doing the PRA check.

To Carl's question, though, we won't -- there is the unknown scenario where you don't know, because it has been forwarded and you don't have quite the confidence. And those are the ones, initially we've said all along that we won't, you know, yes, we will factor all of this into our filtering decision, but that will be the one that will be weighted the least.

The one that actually passes will get maybe a positive weighting and the one that literally fails, I think it was the Go Daddy guys yesterday, and I applaud those guys for literally on the failures not accepting that. For those failures, you bet it will be a negative rating, and it will go into a filtering process, though. It won't be the only thing that we look at. And so we're moving.

So, it's the choice of the implementer. Every implementer will have to determine how they want to interpret that data. And there will be a pass state, there will be a fail state and there will certainly be this unknown state. And that's how we will have to decide to do that.

And then just the second question on what do we do. And, again, I will just oppose a second with Brad, we do move, we don't wait, we are moving, the industry is moving, we have the momentum and we absolutely should move forward on both of these IP and crypto solutions.

MR. SALSBURG: Dave Crocker?

MR. CROCKER: I think that Carl went at something that we would do well to think very hard about: Any proposal has its limits, there are trade-offs in producing them, and frequently the biggest problem with a proposal is that there isn't enough one-hop path registration scheme. And so there must be some utility for that, after all, or we wouldn't be doing that. But the differences in the approach are what's significant.

CSV doesn't purport to be or have any utility beyond one hop. And in looking for which trains to hop onto, I'm afraid I actually think there is more than two. I'm hoping that that doesn't mean that there's a third rail, but that we must have mechanisms for evaluating the operators of MTAs, we must have mechanisms for evaluating the people who inject into that system.

And so it's who should be on the hook, and what are the ways of putting them on the hook that's efficient. And one last comment on that. As people think about what's easy and what's hard. What's heavy and what's light. There's a lot of counterintuitive things that occur. We are all used to thinking about crypto as being heavy weight. In point of fact the computation is not the interesting issue here. Adding software is an issue. Doing administration is an issue.

Some of the schemes that require administration are really simple, but only in the simple cases. They're really hard in other cases. And I'll finish by quoting H. L. Menkin. No, actually, I'm going to quote one more unrecognized engineer. H. L. Menkin said, "for every complex problem there is a simple solution, and declare them both pretty stable.

We need people to implement them. We need some people to start testing. I very much liked that in the panel earlier this morning where -- I mean on one hand we have some people saying, we've got to get going, we've got to make our decision and choose the one and we've got some other people going, it's very clear from our experience we need to do things incrementally.

We need some people to start generating the records for CSV and the signatures for BATV and we need some people to be able to take them on the receive side and interpret them. And so, whether it's -- it can't be one large industry, because there's got to be a sender and a receiver, but we would definitely like to get some players who are willing to experiment with this. If you are interested, please see us after the session.

MR. SALSBURG: Are there any questions, other questions regarding technical implementations of the path-based approaches that would give you pause for concern? How about this gentleman? Right there.

MR. HAMMER: Michael Hammer. My firm contractually partners with a lot of the large players who are here. We send a lot of mail. One of the issues that we have is the time frames as various of the players say, well, we're looking at this, we're testing this, we're going to implement this. And these standards are not necessarily stable at the point they say they're considering them.

And for us to redo our mail systems, it becomes very problematical. So when Carl says on the clear list, well, in our next iteration, we're going to include the hooks or the CSV, we have to start looking at it if he's thinking about using it. And so that's an issue for us in terms of the time frames. And I realize that there's this competition issue, that is the players have interests in not discussing their plans, because it may give them some sort of competitive advantage, but they do have to cooperate with each other.

So, it impacts third parties like ourselves. Now, we have the technical resources, it's a timing issue. With the smaller players, it becomes a lack of resources and understanding of the issues and how to do it. So, they get blind-sided by the timing issues as well. So, my question is, how do we resolve these issues so that the people who are on this world cup tour, who are really the main players, can create some more transparency for other people who can't come to every one of these? Yes, publishing a train schedule.

MR. SALSBURG: I guess let me begin with kind of a question that goes to one of the premises of the question, which is that because of competitive pressures, there is a reason to withhold data from one another. Is that really the case? You all are offering -- those of you that have released licenses have offered royalty-free licenses, it's unclear on its face how any of you intend to make money off of this. Is there really competitive pressure here that's keeping you from sharing information?

Ryan.

MR. HAMLIN: So, one of the things a few years open, we've been talking obviously to these guys and I probably talk to -- I jokingly say I have the best relationship with AOL probably than anyone at Microsoft because I talk to these guys all the time, and they know that. And the same thing goes with Brad. So, we've been I think very cooperative in sharing information and for us it's never been a competitive issue.

MR. SALSBURG: And Brad?

MR. GARLINGHOUSE: I mean, first off, as I think everyone here knows, Yahoo! has definitely taken an approach with the defensive patents we've filed around DomainKeys that they are absolutely open source, sublicensable, we are in no way, shape or form trying to make money through championing DomainKeys. We're championing DomainKeys because we think it's a better solution. It's not to say it's the only solution. I agree there aren't just two trains, there's cabooses and pieces of all these different trains. You started this analogy. So, you know, that is definitely the case.

I think while everyone shares the common interest of sharing this unique user pain point, and certainly when I look at Yahoo! and how we all at v mo T useoc292.8000 TD(18   pieces of all these differen compete. And I think the challenge is that we don't agree on what the best solution is. And, you know, Dave Lewis said earlier today from Digital Impact, you know, players want one solution, they want the best solution. And that's a challenge for us, because we don't agree on what the best solution -- well, I think we agree what the best long-term solution is, we just don't agree on what the timeline is that we can get there, by which we can get there.

Margaret Olson earlier today talked about that people are worried about the cost associated with a crypto solution. I'm worried about the cost of saying, okay, we're going to implement one solution now, but we all acknowledge that there's a second solution that we're going to go do later on and we have to go through this, you know, we're going to have back here, more

Sendmail, I mean every MTA vendor is going to do every one of these protocols. There may be a couple of the open source guys that takes a while to get on the train, but -- have fun -- but the reality is is that the MTA vendors, the people actually delivering this, there's no differentiation. We're going to do every one of them. There's no other competitive choice.

MR. SALSBURG: So, the interests here are to share the data you get when you do testing and work on this collaboratively.

Because of time constraints, why don't we turn to implementation issues that you all may have with the crypto approaches. Anybody have a question or thought on that that they would like to throw out at Jim or at Brad?

MR. JUDY: It will be quick. This is probably very basic and reflects my ignorance, but I don't understand from what I've been hearing how the crypto approaches work in countries that simply won't accept that kind of technology, and therefore I don't understand how it meets the international needs.

MR. SALSBURG: Meng?

MR. WONG: Can you name a country that doesn't allow signing?

MR. JUDY: That's not what I said. What I said is I understood from some of the discussion earlier today that there would be resistance to the crypto solution in some countries because it would permit persons who were political dissidents, who were desiring to hide themselves from their governments to be able to -- there would be resistance to implementing those technologies for that reason. And maybe I misunderstood. If so, I would like to be helped.

UNIDENTIFIED SPEAKER: It was said but whoever said it was wrong. I would like to know your views.

MR. SALSBURG: Let me expand upon the question. What types of dealings have you had with foreign ISPs and operators of mail servers in foreign countries to see how willing they are to participate in any of these schemes? Let me throw it out to everybody.

Jim?

MR. FENTON: So, I don't have any direct experience with what the foreign regulations are, but I think this is really just an example of one reason that people will have that they don't implement signing, and I think we've got to be prepared that not everybody is going to sign messages, that there are going to be legitimate unsigned messages and we just need to be prepared for that. And this is one of the motivations.

MR. SALSBURG: Brad?

MR. GARLINGHOUSE: Just to use Yahoo! as an example. I mean, Yahoo! Mail has well over 100 million active users all over the world. We have hosting in countries all over the world. Obviously British Telecom is an example where we have a sister relationship, one of the largest ISPs in India has already implemented DomainKeys. I question the premise of the question, in that I know that was talked about earlier, so I understand the question, but I don't think there's a real fundamental issue here.

We also had a gentleman talk early this morning about how much -- what really is restricted in terms of encryption technologies and to which countries and to what level, and I don't think the premise of the question is actually accurate.

MR. SALSBURG: Are there other issues regarding the crypto approaches that you would like to have addressed?

me. Where would I get information about all of this stuff?

MR. SALSBURG: That's a very good question. If you are a business owner who sends email or if you run a small ISP or you're a small email service provider, how do you figure out what to do with all these varying standards? Is there going to be one single wizard that somebody can use that will put everything in the DNS record?

Ryan?

MR. CROCKER: There is a place to make some money.

MR. HAMLIN: So, we have done a couple of things. We recognized up front that there was some confusion around -- particularly around creating the SPF record, so we built a little tool that actually is out on the Microsoft.com for Sender ID, and it's a tool that's very easy for any administrator to go through and plug in their domain and put in their IP addresses and it actually generates the exact text and then all the administrator has to do is cut and paste that into DNS.

So, we have made it very easy. And I think Meng has a tool on his site that does it as well. When it comes to generating your SPF record. I know TRUSTe put together a site right a couple of days before this

Summit that kind of listed all of the websites in this email authentication space and has pointers out to each of those sites. So, there will be a pointer to Microsoft, there's a pointer out to DomainKeys. So, if you go out to TRUSTe's site, that's probably a good central place to start and it will give you the links, pretty much, to go learn more about this.

But I totally agree, there has to be a simple way to do this and that's why we built this little tool and put it out there.

they have to get techies to do for them at various locations in their lives and stuff like that, and it would be good to know where to start looking for some of this information.

MR. FENTON: Sure. Well, with the cryptographic approaches, one of the really nice things is that the signing and the verification can happen anywhere in the path between the sender and receiver. So, it's possible that your, you know, as perhaps as a premium service, that your Internet Service Provider or your domain registrar could provide the service of signing messages for you, you send your messages through them, and they, you know, generate a key on your behalf and advertise important point. Could there be wide scale adoption of any of these proposals? People who aren't the techies of the world have to be able to use it. Are there things that can be done other than publishing a tool that an administrator person would know what to do with that?

I gather from the question, you know, cutting and pasting, it's nice to say, but cut it from where, paste it to where? And how do these -- how can you accommodate people that don't have the technological savvy that Carl has?

MR. CROCKER: By the way, do you think of that as a high or a low bar?

absolutely right, and I think we need to make it easy for everybody, and the Barbie doll example is a good one to think about, I just think that the reality is those users -- that category of player that's using somebody else's commerce engine, somebody else's tools and hosting, you know, they're going to use that provider's.

MS. RIVERS-BAKER: But they're still going to want to know about it.

MR. GARLINGHOUSE: They just want to know that it works. They don't need to know how. I mean, my mom, if she's doing a Barbie doll site.

MS. RIVERS-BAKER: Some of them do. They might not need to understand the technical stuff, but once again, there is a certain category of micro business owners who they're enough of a control freak that they're going to want -- at least want some information about it. You know, they might not need to -- they might not need to feel like they have to dig into their own zone files and figure all this out from a technical

You know, if you use the person who is selling Barbie dolls, they are people like my mom. And she has no idea -- this conversation wouldn't make sense to her. She doesn't want to know. She just wants to know that when she sends a marketing message or a confirmation of transaction message that it gets through. If it doesn't, she's going to call that vendor, that provider and she's going to say, "hey, it didn't get through, what's wrong? What can we do?" And they're going to say, "here's the problem, I can fix it for you."

MR. SALSBURG: Jim Fenton, let me give you a follow-up question. You had said that one of the things that would help a person who is in the business of sending email regarding Barbie dolls is their ISP could offer premium service, which would include the publication of the cryptographic record -- of the DNS record. Is what we really want here universal authentication? Should this be a premium service, or should it just be part of the standard deal you get when you sign up with an ISP?

MR. FENTON: Well, of course as a customer, I would like it to be part of the standard deal.

MR. SALSBURG: But as a person who is trying to put forth a standard that -- I mean, the more becomes. Is there a global interest where ISP should say, we're not going to make money off of this either?

MR. FENTON: Well, perhaps, although there are certain, you know, there are lots of domains around that are not used for sending mail at all. That are used maybe to host a website or something of that sort. And, you know, there is some additional work for the ISP involved, or whoever is doing this. So, I guess that was on that basis that I said it could be a premium service. But, you know, that's one of those things that I think the market is going to decide whether it's a premium service. If some ISP or some domain name registrar started offering the service for free, and was still able to make a buck doing it, then the market would probably vote with their feet in that direction.

MR. CROCKER: Yahoo! offers for free.

MR. SALSBURG: And how about Cisco?

MR. FENTON: Cisco is neither an ISP nor a domain name registrar.

MR. SALSBURG: Sana?

MS. OLSON: So, I actually think the answer is somewhere in between. I think that you're right, most small businesses don't care about the details and won't want to know. In fact, I once was trying to describe a little bit about authentication to someone who said, oh,

sending point to point from, you know, their bulk email servers, and it's a very simple modification for them to add this DNS record for Sender ID or for SPF or for CSV for that matter and, you know, have it interpreted when it gets received, but that's not -- it's not quite as, you know, a slam dunk, let's go ahead and implement it for users, who are often sending from many different places, they're sending from their work, from their home, they're roaming, you know, they're at a Starbuck's on T-mobile or something like that, and for those approaches I think crypto works much better, and I think in the long run, it might gain better acceptance, you know, from more than just bulk emailers, and sometimes I wish there was some way that we could better represent, you know, what the average user on the Internet and what their needs are at this type of a panel. So, I think the crypto approaches are perhaps a better long-term solution.

MR. SALSBURG: Doug?

MR. OTIS: With respect to going to crypto, I think you're right. And as was pointed out in other countries, they don't have, necessarily, the network bandwidth we have, and are much more sensitive to the network infrastructure and that they're running a school off a T-1 line and whatnot. But they are sensitive to that, and that's something that the crypto schemes do not protect you. In other words, you're still going to have to digest the entire message, analyze it and decide no, this isn't what we want.

And that's where I think you'll see that CSV which is also capable of running a reputation service comes into play. And I think you will always see that you will need CSV and some kind of encryption scheme off into the future, and it's that subject that I am very adamant about, that we need to move on both of those issues.

MR. SALSBURG: Dave, is BATV stuck in the station, or is it hooked to a train or is it about to get hooked to a train?

MR. CROCKER: BATV was another item where we sort of wandered through parts of the standards process and got shuttered off to a side track and let's not do that image. The reality was we were slow in doing a competent spec. We put something out very quickly that was more a description of an idea, but I have been quite astonished at how much mind share it's gotten given how bad the writing was. We're starting to get some people talking about implementing it, one of the nice things is, especially when you're doing the private key is it takes a decision by one entity to implement and you don't have to rely on anyone else.

Some people are playing with different algorithms, I'm particularly interested to see the one that Tony Finch in Cambridge is coming up with. So, I think that a number of things that look like they're stuck 6   stuck 6   stck 6 7fw dl1.0ke-2hts go is t,:lki000 TDle

MR. SALSBURG: Let's shift gears here for the balance of this panel. Obviously when you leave here today, we want you to do something, otherwise we wouldn't have called you all together. And our hope is that when you leave here, the testing that you've already begun continues in earnest. For those who haven't started testing yet, the testing is going quickly, and we see some results.

Now, the question I wanted to direct to the panel is, have you already established testing protocols? Have you designed your test to see not only do they -- how do your systems affect different types of users, both senders and receivers and intermediaries, but how do they interact with other -- the other schemes that other people up here are working on, and are you in a position where you need to get additional volunteers to assist in the testing, and if so, are they different types of users, are they the smaller businesses or individuals?

So, why don't we begin with Brad.

MR. GARLINGHOUSE: So, I mean, the best, and there's been a couple of data points that have been discussed earlier in this event, you know, Sendmail has done some testing to date with regard to DomainKeys that has certainly been very interesting and a good discussion yesterday about testing that ColdSpark had done, and in our own usage, you know, we are of course monitoring, I don't deny that there is some overhead associated with a crypto solution, you know, that know, players ranging from EarthLink to, you know, we're seeing enough interest that while we would certainly welcome a broadcast of, listen, if people are interested in testing DomainKeys and interfacing directly with us on those tests, great, let us know. You can email me and we can get you in contact with the right people.

There's certainly no -- we're seeing that there is interest and that's good, and so there's momentum. The more the merrier.

MR. SALSBURG: So, for there to be widespread deployment, it's going to have to be more than just the large ISPs that are participating. Is there a benefit now to soliciting some of the smaller players to see if they would participate in your testing?

MR. GARLINGHOUSE: Well, so one of the things that we're, you know, as we look at it, and really AOL set the I think benchmark around this, at some point we will probably say, okay, you know, we have over 100,000 IP addresses on our whitelist, and if you want to remain on our whitelist, you need to start using DomainKeys. And we don't want to do that today, but it's certainly something that we look at as likely to happen, and we do want to have that testing done with enough unique cases and small enough players before we did that that we wouldn't cause disruption for anybody. But there aren't

never be kind of the end of the testing phase. I truly believe that we're happy to turn it on live and start to use it and then over time as we feel more and more comfortable, we will crank up the filters and that input will be even more valuable, but we will never stop testing, because the spammers are going to figure out different ways to get around it.

MR. SALSBURG: Is most of your testing right now based on Hotmail? Are you testing mail forwarders?

MR. HAMLIN: Well, I mean, so mail comes to Hotmail via forwarders, right, so we -- yeah, by default, we are -- that's why a lot of those case studies that you saw, Harry has, that was just a small sampling that he talked about yesterday, we've got a full list of if X happens and Y happens and Z happens, here's what that record looks like. Did it pass, did it fail, or is it unknown. R?s0 cm0.00 0.0e get amlL0000gu6.TjE0 0.0

MR. CROCKER: Yes.

MR. SALSBURG: If you could have the perfect test partners, what would they be?

MR. CROCKER: No, everybody would be overwhelming, that would be a success failure. We need some people who can implement the code on the sending side, the receiving side, some people who are comfortable enough playing with algorithm variations that we can tune different choices for the encryption, and people who perhaps have enough incoming or outgoing flow to make the test interesting.

MR. SALSBURG: Is there anybody in the room that would like to participate in a test of BATV? Okay, I see AOL. I see Yahoo!.

MR. CROCKER: There's a meeting tomorrow morning I would like you to come to.

MR. SALSBURG: Well, I can get it all on the record right now, we have a court reporter right back there.

MR. CROCKER: Please raise your right hand.

MR. SALSBURG: This is great. You know, Dave, is your email address anywhere? Do you want to give it out publicly?

MR. CROCKER: Oh, heavens. Oh, heavens, more spam. Oh, gee. Somebody was talking about getting

2,000 messages a day that was spam and a couple of us looked at each other and said, that's pretty low. D. Crocker, D-C-R-O-C-K-E-R @ Brandenburg, B-R-A-N-D-E-N-B-U-R-G .com.

MR. SALSBURG: And Doug, testing, are you in need of testing partners?

MR. OTIS: Well, we are not really developing mail transfer agents. Our specialty is reputation. Sorry. Our specialty isn't really developing MTAs. We've fiddled around and we've made our own modifications to our mail servers to look to see if we weren't off the mark and what we thought could be done. However, to deploy this and get feedback on the community, I think we have to depend on the community helping us. We do have a reflector that can be used. There's an easy to remember link to it. Can I give the website instead?

MR. CROCKER: Yeah. Well, CSV absolutely would like testing on the same basis, except not to write code. Well, some of that, too. Anyhow, the place to go for both CSV and BATV in getting some information, and I have to upgrade the web pages tonight, but which we will, is MIPASSOC, which is M-I-P-A-S-S-O-C, .org/clear, C-L-E-A-R.

MR. SALSBURG: And Jim? What's Cisco's testing regime right now?

MR. FENTON: Sure. Well, we have a few domains that are signing right now with Identified Internet Mail, and also checking as well. And we recently published an open source reference implementation, which is available on SourceForge, and there are a couple of mailing lists there as well, for discussion and, you know, please let us know how it's working for you and all that sort of thing.

I think the testing is an extremely important aspect here. Really the measure of really any of these systems is that the measure is really not the number of people that are signing or the number of messages that are signed or the number of places that are publishing particular kinds of records, but the measure is really how well000atwbut the 36.00wn eallfRti000a000 0.0000gRti00I8i00 1.

that, you know, as a whole, all of us could probably do, in terms of developing systems that people -- allows people to, with appropriate anonymity, share the results of their testing so that we can get some more centralized data about how these different mechanisms are working.

I know there's some organizations like I believe that MAAWG is doing some testing of -- or collecting some test results from some of these schemes. But in general, because of the proprietary concerns, the -- a lot of these results aren't public, and what we need to do is figure out what it takes in order to -- anonymize these results so that they can be shared publicly.

MR. SALSBURG: Is the concern that the results show who the senders and recipients are, versus whose proposal it is that's being tested?

MR. FENTON: Yeah, it's, I think, more of a matter of -- and perhaps somebody that's more directly involved in the testing effort can clarify the motivation, but yeah, if two domains are exchanging a great deal of traffic, it might indicate that some transaction is about to take place.

MR. SALSBURG: And when you say MAAWG, you're referring to the messaging Anti-Abuse Working Group?

MR. FENTON: That's correct.

MR. SALSBURG: Is that the appropriate forum for sharing test results here and making sure that everybody knows what's going on with each other's protocols?

MR. FENTON: Well, like I said, there's a limited amount of sharing that they can do because of the way that they're structured right now. And I guess I'm a little bit concerned that they don't adequately cover all of the use cases involving enterprises and all these things, it's primarily a group of service providers and people in the mail business.

MR. SALSBURG: How do we go about making sure that your testing data that you all obtain in the next couple of months is shared widely with the technical community so they can see how these different standards that you're proposing are functioning?

MR. HAMLIN: I think there's a couple of things. One, we've kind of done that throughout all of this, obviously the IETF process was a great forum to do that. Now that that is no longer, we come to things like Inbox next week and other opportunities to kind of share this data. We certainly will be -- can publish that and also some of our findings out on our site as we get those, and I think it becomes more interesting as we're obviously live, and we can start to really show how many -- there's a lot of sources of information around.

I know Meng has some data on his site where he talks about a number of domain publishing. So, if we can just leverage kind of the existing sites that are already there and just start to publish more of this information than just sharing it publicly.

MR. SALSBURG: Going forward, would all of you on this panel agree that you would share your data, your testing data?

MR. GARLINGHOUSE: Yes.

MR. HAMLIN: Yeah.

MR. CROCKER: You bet.

MR. FENTON: Sure, we do need to clarify a methodology for collecting that data from, you know, not just from our own domain, but from other people that are using IIM.

MR. SALSBURG: We have a question in the front row, if we could get a microphone.

AUDIENCE MEMBER: Thanks. Steve Warren, Educall [phonetic].

So, with respect to the testing data, one of the more frightening things that I've heard, is that at least Microsoft, and perhaps others, at some point are planning to drop, just sort of discard as absolutely invalid mail from domains that publish SPF records which haven't come from that MTA. And that will immediately break a lot of the forwarding and a lot of the listservs and a lot of the people who are sitting with multiple accounts, just using their local ISP for routing, that will immediately break them, but they won't find out that it's broken until the day that you start dropping them.

And so, but you will know the day before, from your testing, how many thousands of messages a day you will be dropping. So, I just wanted to put in a pitch for when you do the testing and share the information, you let someone, maybe the FTC or the rest of the world know how many messages per day you will be planning to drop the day you start dropping them.

MR. HAMLIN: Yeah, I think -- I mean, the case you're getting to is whether it's a direct mismatch, where it literally fails, where we can feel with confidence that, you know, this mail says it's coming from eBay, but it does not match the IP address that eBay has published, should we continue to deliver that, should we put it in the inbox, should we put it in the junk mail or should we delete it all together. And the question is will we ever get to a day where when that fails, then that one criteria alone, is that going to be enough to just delete. And I think we've been very clear all along that there's an input process, all of this is an input to the filter. And the filtering process today is about 90 percent effective. And the way you get your filter better is you give it more and more data points. And this is one of many data points that we will put into our filtering process, and that the process -- I mean, the thing that hasn't been brought up today is the reverse of deleting the mail. There's goodness in protecting a lot of the brands that exist. I mean, we talk to people like eBay and Amazon and there's a bunch of people here that aren't even represented that care a ton about their domain and protecting it and making sure that when a mail comes from eBay, it matches. And so we're going to have good ratings, too. It's not just the negatives. We're protecting the brands of those good domains that want to make sure that they don't want to be spoofed anymore.

AUDIENCE MEMBER: But nonetheless, to say it again, you will know how many of these forwarding and mail serves and lists and all of those other things that we recognized that the filtering doesn't work with, you will know in advance, because you say you're looking at them.

MR. HAMLIN: Yeah.

AUDIENCE MEMBER: So you will know which ones are actually forwards and listed?

MR. HAMLIN: Yeah.

AUDIENCE MEMBER: So, that's part of the data that we should be getting, and that's the point.

MR. HAMLIN: Yeah.

MR. MENG: I think I see where you're going with this question. I would like to ask the audience a question. This is a little thought experiment. So, let's pretend that we have a sending domain and you're the receiving domain, all right? Let's pretend that as the sending -- let's pretend the sending domain does two things. They publish SPF records, and they sign all out-going mail, whether it be with IIM or DomainKeys.

Now, suppose you are the receiver and suppose you do two things. You check SPF and you check the signatures, okay? So, we've got complete compliance on the sending end and on the receiving end for SPF and DomainKeys. Now, suppose that domain has announced, "we always send all mail through this set of servers, so the SPF is good for that, and we always sign all mail that we send out."

Would you be confident if you got a message that did not have a signature and did not come from one of those servers, would you be confident in rejecting it?

(Various answers.)

AUDIENCE MEMBER: Who does it say it's from?

MR. WONG: It says it's from that domain. Sorry, that was a trick question. So, who would be confident receiving that message? It's from some other IP and is not signed or the signature looks like it's broken.

AUDIENCE MEMBER: I was going to say, there's a timing issue too.

MR. WONG: Suppose two years from now. Yeah?

AUDIENCE MEMBER: And everyone is publishing and everyone is signing?

MR. WONG: Everyone is publishing and everyone -- well, just that particular domain. That particular domain.

MR. CROCKER: I would really like to hear why Carl would say no.

MR. HUTZLER: It's not that I say no. I don't have the data yet to know, and this gentleman here, I forget your name. Steve, he mentioned earlier today or yesterday that he has five accounts that he sends out through RoadRunner or Comcast, and neither SPF nor DomainKeys will allow for that, unless he's doing direct signing of his mail in his MUA.

AUDIENCE MEMBER: You agree that you were doing the same thing, by the way. Just to be clear, it's not a weird odd-ball thing.

MR. HUTZLER: I actually am a spammer. You didn't realize that.

MR. SALSBURG: Is that on record?

MR. HUTZLER: The question that Meng asks is would you feel comfortable, would AOL feel comfortable doing that? I guess at some point you have to look at 0.00001 percent, and you have to make a decision at that point. You know, until we have numbers from some of this testing, we won't know, but, you know, at this point, it's a really tough thing to make a call. You know, you have to start doing something at some point.

One of the things that I think AOL is thinking about is if large chunks of mail can be confirmed or verified according to Sender ID, DomainKeys, IIM, even CSV, if we can get some or all of those to check out, we probably like that mail a lot better, even if it ends up being spam, because again, like I said yesterday, a lot of our spam is coming from other ISPs, some of which already sign with DomainKeys and it checks out. But the key is that we can now base reputation on that domain and we can talk to that ISP or that provider. Even CSV, you know, CSV is really a direct way to do that. But, you know, we're always going to have that potential for false positives, if we get it down low enough, I guess that's where we might feel comfortable rejecting the others. It will be a while. It may be in testing, I don't know.

MR. SALSBURG: Well, unfortunately we have just missed about three minutes of our cookie time. So, I apologize for that. But I want to thank the panel for sitting up here and fielding questions and I also want to thank all of you for your good questions.

(Applause.)

MS. DREXLER: Okay, everyone, we're going to get started on the last panel. I know this is the last it's come up numerous times throughout the summit. So, we're going to be discussing that. We're going to explore it in depth. We're going to talk about why many feel this is what's necessary and we're actually going to learn about some of these things that are already being done to help provide accountability in the email system.

Specifically, as I said, we're going to talk about reputation and accreditation, challenge response and other types of approaches that are working to reduce the spam problem.

I just want to point out, both to the audience as well as to our panelists, we're not going to be looking at the pros and cons of any particular approach, instead we want to just talk generally about what's out there and how they can work either on their own or, and/or with email authentication.

Now, to give you an idea of what our layout is going to be, first we're going to discuss challenge response, then we're going to discuss some unique approaches, one of which is going to talk about a variation of challenge response in combination with tokens and whitelisting. Then we're going to discuss an approach called Email Sender Verification, and then we're going to move on to reputation and accreditation and other approaches that will help set the framework for accountability in the email system.

Panelists will each be given a little bit of time to overview their approach and then we're going to leave lots of time for question and answer from the audience.

First, what I want to do is introduce our very large panel. First we have Stephen Currie who is the Director of Product Management at EarthLink. Then we have Daniel Burton who is the Vice President of Government Affairs with Entrust. Then we have Clemens Perz, the CTO of All About It. Then we have George Mattathil, the CEO of the Strategic Advisory Group. Next to George we have Fran Maier who is the Executive Director and President of TRUSTe. Then we have Craig Taylor who is the VP of Technology at IronPort Systems. Then we have Des Cahill who is the CEO of Habeas. Then we have Tonny Yu who is the CEO of Mailshell. On Tonny's left is Richard Gingras, the President and CEO of Goodmail Systems. Then we have Meng Weng Wong who we are all familiar with. He is from Pobox.com. And then next to him, last but not least we have Hans Peter Brondmo who is an entrepreneur and Fellow with Digital Impact.

You will note on the agenda, there were two other panelists who were supposed to be here, Karen Wendel of Identrus was unable to make it and likewise Ray Everett-Church, which I can understand because I'm feeling that way myself, has come down with laryngitis and is not able to be here. So, our panel is large enough, though, and I don't think that will be a problem to have two less panelists.

So, we're going to get started. We're going to just go down the line, the panelists can come up to the podium if they have a presentation, so we're going to start with Stephen Currie who is going to discuss permission-based systems also known as challenge response. So, I'll turn it over to you.

MR. CURRIE: Thanks, Sheryl. I always knew that this was going to be the most scintillating panel, so I'm glad a lot of people stuck around for it.

First I want to thank the FTC for putting this together and giving us the opportunity, all of the panelists over the past couple of days and certainly the audience. It's been a very rewarding two days. I've learned a lot, and I look forward to seeing a lot of the things we learned put into the market and put into action.

This panel was billed as beyond email authentication, or the role of reputation and accreditation systems, sort of the next step to authentication. I kind of wanted to offer a slightly different perspective and talk about something that's been in place for a while now and how it really acts as a reputation system that's individualized to each user, and that's permission-based systems. EarthLink calls it permission-based systems, the industry a lot of times calls it challenge response.

But Earthlink has had a permission-based system in place for about 18 months as an opt-in to our customers, so I wanted to talk a little bit about what our observations have been with that and how it's, as I said, in a sense a reputation system.

First I'm going to assume everyone knows what permission-based or challenge response is, but I'll just go over it at an ultra high level. A user maintains an individualized whitelist which is generally their address book that's tailored for the user. Any email that comes in to them from someone that's in their whitelist or in their address book gets delivered right to their inbox.

Of course, the first question everyone asks is what about that serendipitous email that I wanted to get from someone that isn't on my whitelist. And that's where an auto response mechanism kicks in, so it sends an auto response back to that user asking that user -- telling that user they don't have permission to email them, asking them to fill out a simple form to request permission to email them and the user can decide for themselves whether they want to get email from that person or don't want to get email from that person.

There are several ways that you can get emails that are suspect. I won't go into all of them, but the main mechanism is that it's the challenge that the person fills out, which is in a sense a reputation system. Someone brought up yesterday making email a little bit more like instant messaging, and this is one way to do that, if you think of subscribing to someone's presence, and you have to ask, or you have to have permission to subscribe to someone's presence, and this is really akin to doing that.

So, why is this similar to accreditation and reputation systems? And I'm sure a lot of things you're going to hear about today. In a sense, it really changes the paradigm of email. Right now, most of our email is set up to accept everything, and then we spend a lot of time trying to filter out the bad stuff. This

I'm going to deliver that right to my inbox. So, making that fundamental shift is very important and has been very valuable to a large set of customers that are willing to do that.

Where it's different from a lot of reputation and accreditation systems en masse is that it's tailored all got the email that we know is good, we've all got the bad email that we know is bad, but there's this big section of email in between that is good to some people and bad to some people.

Someone brought up Amazon.com yesterday, I think it's a great example. A great example. Amazon.com by any measure is going to be labeled a good emailer. You know, they're trusted, they provide a valuable service, they're not hiding, they're not trying to obfuscate who they are, but I really don't want those 10 percent off coupons, you know, once a week or however often I get them, and I think those are spam.

So, one thing that permission-based or challenge response systems can do is really put a user-defined system in place so that they can make decisions for themselves and have their own personal reputation system about what they think is good and what they think is bad.

Just a couple of quick caveats that I wanted to get out. First of all, it's not for everyone. You know, there's a large set of use cases that permission-based email systems aren't going to accommodate. And if you're looking for a job that a lot of business applications where you're dealing with a lot of people you haven't had contact with before, permission-based systems probably aren't the right thing for you.

Also, it doesn't -- they're great for consumers, but they don't do anything to address spam on the network level. You know, an EarthLink customer who is using this might be very happy and might not be getting any spam. EarthLink is still paying to have all that email come in, process all that email and deliver it to the customer. It's only at the very last stage that the customer says, "I don't want this to come into my inbox."

So, it doesn't do anything to address the network level of spam, and in a small sense, it may even contribute to it a little bit in the sense -- or contribute to the overall email volume a little bit in the sense that it's sending the auto responses back.

And the third thing is, they work very well when not delivered en masse. If and when permission-based or challenge response systems become extremely prevalent and everyone is using them, it is going to raise a unique set of issues about having to whitelist each other's challenges and things like that. I'm quite sure that all those issues can be overcome, but I wanted to point out that it does raise a set of issues.

So, I just wanted to quickly summarize in saying that permission-based -- from EarthLink's perspective, certainly, permission-based email or challenge response has been a fantastic pseudo reputation system for our customers. One of the issues up front was was it going to be too complicated and it hasn't been. It's amazing

Authentication," and the "other tools" part, because I really think that's where the solution that I'm going to talk about comes in.

It is not an email authentication solution yet, although we may morph to that. It is more a web access authentication, antiphishing, how do you stop sort of identity theft, or prove identity on the Net. And as we looked at the solutions out there, we sort of had a very simple curve, and there's a user name password, and then there's a big gap and you sort of jump into things like digital certificates and secure tokens and PKI and encryption.

And we thought, what is the simple authentication, the online identity second factor authentication that it seems like the market is crying out for, but yet somehow the industry is not delivering, that can address some of these questions about identity on the Net and specifically identity theft and phishing.

And so, we came up with a challenge response system, it is a second factor, and I'm holding that second factor in my hand. It's a piece of plastic. It is a token, but it has no electronics on it, there's no chip. If I leave it in my jeans through the washing machine, it's not going to hurt it. If I step on it, it's not going to destroy it. And so what is a very simple challenge response system that can allow users to authenticate themselves securely into websites and so this really addresses the transaction-based more consumer confidence crisis that I think one of the earlier panelists talked about on the web.

So, the solution that we have, challenge response solution, is say that you are a bank, and your customers are very concerned about doing secure transactions with your bank, and user name password is getting phished, or getting hacked. I think about 20 percent of user name passwords are broken is the data that we've come up with. And so what's a simple second factor that would prove your authenticity to that website so that you could then go in and securely do your transactions, whatever.

And so we came up with a product that's called Identity Guard. It is a piece of plastic, backed up by a software program run with Java that runs on a Linux server, and the easiest way to think about this Identity Guard is bingo. And I know that sounds trite and trivial, and I think in a way it is, but in fact it does deliver a very secure level of authentication on the Net.

So, each customer of the bank would have a -- would be issued a card like this. When you get into volumes, you really get down to pennies a card, so it is not an expensive second factor. The card has a grid inside of it which would be unique to each user. There are numbers across, letters across the top, numbers down the side, and then when you enter your user name and password into the site, into your banking site, for example, they would then prompt you with some grids, and the prompt would be, what is in grid A-2, B-4, C-5, and you would then look on your bingo card and you would say here's what's in A-2, here's what's in B-4, here's what's in C-5. You would then enter those in, the software package would match your user name and password with that unique grid and give you access. And every time you enter there would be a random generation, so there would be a different set of prompts every time you signed into your account.

And I think the other part of this second factor is it's inexpensive, it's easy, intuitive to use, it's easy to deploy across systems. If you lose it, it's not hard to replace, you can just call up and put a stop to it. It's easy to distribute and deploy, you can either do it in the form of a card, you could do it in the form of a perforated set like this on a bank statement, you could stick it on the back of an ATM card, you could stick it on the back of a credit card, you could stick on the back of your health card. So it does have a great deal of flexibility.

It's also flexible to the extent that the enterprise wants to ramp up the security. So, if you have one grid, now it's a one in ten chance of breaking it. If you go up to the three or four, you get into the hundreds of thousands or over a million of random possible combinations that you can have here, so it's an easy way to stop brute force attacks and you can simply lock people out if they try to guess three times and don't get in.

So, it is sort of a high-tech/low-tech combination, it's second factor and it's a way that we try to think about what is something that's really preventing the secure kinds of transactions and communications on that ad. Because not only are consumers, but increasingly enterprises are very weary of who's getting access to the sites and who they're going to be doing business with.

So, like I said, I think that is beyond email authentication, it clearly falls into the other tools category. I had a demo which sort of showed this in realtime, if anybody wants to talk to me afterwards, I would be happy to go over it with you.

MS. DREXLER: Great, thank you.

it and I think I will just go into it and present the core idea of it. I'm not going into all the details now. There have been a lot of nice ideas what else could be done with this.

So, having a quick intro, there is an idea of deciding what is spam by just an easy rule which comes from the challenge response systems. So, I decided to talk to someone who sent me spam, that is what usually is the case, but if I don't know him, he can introduce himself. This is something that we really know from each conversation that we have. If you try to enter a house, there is a door that you have to cross, you press on the bell and something happens that you can introduce yourself and someone may let you in. So, if you come more often than just once, then this process will be very short in the future.

For the first we all might think about the user-based whitelist. These are the addresses of people of -- these are email addresses where I accept mails from. And the second thing is something that we have -- well, that's why I say that's unique to Spamkiss and the way it does it. What Spamkiss has here is the so-called Spamkiss token. This is just a pretext edition to an existing email address. So, it's really bound to that address, you cannot disrupt it.

It's chosen and managed by the user himself. If the token used by the sender his relative address will be added to the recipient's Kisslist which attributes to the fact that you only read it once and you send your first message.

I'll give you an example of what this token works and looks like. I think of John Doe who is a developer working with the Spamkiss team and he loves eating sushi. So, his email address may be JohnDoe@DEFSpamkiss.com. And if you put the token in, it looks like that, JohnDoe//sushi-spamkiss.com.

So, the easiest thing is that having the email address of John Doe does not entitle you to send messages to him, but also having the token, which if he would be here, he could hand it over with his email address easily, or if you come home, you can just start writing email messages to him, without bothering that there is a Spamkiss system in between. There is no knick-knack with emails getting back and forth with any challenge response stuff.

Spamkiss has started as a mail module, which means it's inspecting SMTP information as it occurs, while the message is arriving. After the recipient decides to accept or deny the message, the sender will always get a failure notice from the sending MTA, so you are always sure if your message has gone through or not, because otherwise if it's not gone through, you have an error message. We look through the conversation. Well, this is something for the boys, waiting for it all the time.

So, in the SMTP, we will have a greeting, and then the helo thing, which there has been a lot of talk about that, then some step that will be -- that the sending MTA states from whom he's wanting to send messages. So, we know now who is doing it.

In the next step, he will say to whom he wants to send the message. And this is the pair, who to whom, and at that point, Spamkiss may decide to reject the message. Before anything arrives in your network, well at that point, the user can say, do I want Spamkiss to reject the messages or do I want it just to flag them? So, it adds an additional header so that he is able to move it into a special folder with his email client.

Or perhaps saying, okay, this is someone I don't know, the header is named Ishmael Claz [phonetic] and the flag will be unlisted at some point, so if it's someone I don't know maybe, I just send them through my usual spam filters, but only if he's not on my list.

If you are using the Spamkiss token, it must be added to the user's addresses by the sender in writing his first message. As I said, you only need it for the first time. An email address with a token is still an email address. So, that means you don't have trouble with forwarding. You don't have trouble with other things that are not easy to handle with challenge response systems.

For instance, you order something at Amazon.com, you just give them an email address with a valid token and they are always able to reach you. We added SPF to Spamkiss to secure the addresses that you have on your Kisslist, that means on your whitelist, so you can selectively say, I want to check Amazon.com against SPF, but I don't do it with others. That means if you have friends having their own domain, never will it be misused perhaps by a spammer, you just turn SPF off, or you say I do not forward them. It's always the user deciding that.

And you always have to see that the first message is also a valid message. You can write everything in there, you add the guide to your address book, and then you write the first message, just adding the token for the first time and then the next time you just use his normal message -- his normal address.

I would do some steps to a second one, which is just as successful, I think. And I also would like to point out that for outgoing messages, Spamkiss is also there checking to whom you sent messages to, adding the receivers of these messages to your Kisslist so that they will be able to answer without any -- without any delay or without anything going on in between there. But also you can -- for instance, you can have an end token which might be a special token that you can define, and you exchange for outgoing messages, you just exchange the envelope address of the sender with something containing the token. That means if something goes wrong, and you get a DSN from some MTA, he will send that to the envelop message, and that contains the token.

So, there is no trouble getting DSNs on actions that you took before, because it only happens if you send a message, nobody else will have the tokens. That the MTA at the moment when he generates the DSN, that means you can block all the other bounced messages that you get not containing the token in the email address.

Well, of course, the token is just the text. It's a spring that you can just spread it through many channels. The fine thing is that as I said, in personal conversation, when you hand over your email address to another person, you just give them your token and you're done. And of course you can publish it on websites, maybe you can even have some device generating automatic tokens for any info or order addresses. Maybe these are only valid for 30 minutes. So that means if someone clicks on the mail to link, a token will be generated. This is a valid email address for a half an hour. He can send his message. He will be on the Kisslist, next time you will find any messages from him obviously in your inbox.

There is one situation where it might not be enough that you can handle over tokens personally. That means for instance, at 5:00 in the morning you just finished a report that you want to send by mail and you get an error message saying you need a token. You can't call anyone to ask him for his token. So, there is a website, mytoken.com, which acts as a broker between you and someone who owns a token.

The funny thing about that is you don't need to register there. All the interactions are going through SMTP. So, there is no database behind it, there is no information stored on mytoken.com, everything happens at the time when you request the token from them.

But of course, the user has an option in his Spamkiss account saying, if you want us to allow someone to be able to request a token by mytoken.com or not.

Just a short look at the form that you fill.

First you give the email address that you need the token for. Secondly, yourself you need an email address to receive the token. That means if you use that site, you have to come out of any camouflage and say, here is my email address where you can send messages to. The third little thing is just the humanizing feature saying that no automatic program can use this site to get tokens.

Just a quick look on the way it operates. It must be clear that it is a mail interface saying that you have an existing mail infrastructure and you integrate Spamkiss right away.

For me, I think the most important spot where it will be used, smaller companies that have not the capabilities and budgets to install big antispam systems based on filters, rules and a lot of knowledge. I have seen nice projects installing nice software with teams of ten or 20 people, programmers, geeks, everything. You know? Money wasn't the case. But for many of these small companies, money is really the case. So, if you have your own mail infrastructure, we see that the people interested in this technology are mostly these small companies.

Well, I have to make one statement, because as an economist, I like to point out that sometimes technical possible spots -- technically possible spots

4,000 emails per week, which is spam, which translates into 150,000 to 200,000 per year, which is more than my fair share of the spam. Before I continue, let's get to the presentation.

So, this provided the motivation for me to come up with a solution. Here are the constraints with which I worked with. The first constraint is, email is a personalized communication medium. So, no generalized fool-proof solution can be found after the email is sent and on its way.

The second constraint is Internet design is based on distributor architecture. So, no centralized solution is viable. The solution consists of two parts. The first part is, instead of focusing on the spam emails, focus on the real emails which you like to receive and figure out efficient ways of getting it through, through the system.

The second component is develop antispam solutions to enable email users so that they have automated tools to monitor, manage the use and abuses of their email addresses. The name of the technology is Email Sender Verification System, and it is patent pending. It is a overlay system solution so that during the process there is no need to process the existing email infrastructure. It has a distributor lock feature, so it is consistent with Internet design.

ESV solution is 100 percent effective if both the sender and the user use it. There are no false positives or false negatives. In essence, rather than filtering out spam, filter in real email which you like to receive.

Here is how the system works: There is an email user component and there is an email server component for the verification server. The users download the client system on their desktops, laptops, PDAs, or any email enabled device. The users set up their use policies and usage patterns for their email addresses on the ESV server.

For example, one user may send about 20 to 30 emails a day, where someone else might send 200 to 300. So, that is an example of a user pattern for an email user. And once the usage patterns are set up on the system, the system will automatically manage and monitor the uses and abuses.

Here is how the email transmission will happen: Before an email is transmitted, the verification server is checked to find out if the transmission is compliant with the usage policies and the usage patterns described by the user. If it is not compliant, the email is not sent. The user and their administrators are notified about potential abuse.

If the email is compliant, then a tamper proof ESV tag is generated and embedded in the email. The email is then sent using standard protocols. Now on the receiving side, if the receiver is not ESV enabled, then the email is processed as usual, without any change. It does not need any changes to the existing systems.

If the receiving system is ESV enabled, then the ESV server, or the email receiving system contacts the verification server, the same verification server will generate the tag to check for its validity. And if the tag is valid, then the email is not spam.

If the tag is not valid, then most likely the email is spam. If there is no tag, then the email is processed as usual.

Now, regarding the ESV tag. The ESV tag is unique and different from all other tags and (inaudible) schemes. The ESV tag is processed only by the verification sending verification server. So, no public key encryption, certificates or PKI are required for deployment. In other words, the ESV tag and coding is totally private to the sending verification server. This simplifies deployment issues.

In terms of deployment, as an overlay solution, ESV verification servers can be deployed withoute required for impacting any ofFtheTexiRtecordemaIl.infrastructure servers. Verification can be deployed by ISRr0o5i0re

[illegible]

enabled under the CPM system, then the sender ESV server is contacted in step four.

If ESV is enabled, and the tag is valid, then the ESV can go through the set and the email is processed as usual.

What we are looking for is resources and collaboration to bring the ESV solution into the marketplace, which includes partnerships for developing an ESV standard, development partnerships, distribution partnerships and partners interested in using the ESV further down that might have slightly different views of what those are, so I encourage you all to discuss those differences as well. So, whenever you're ready, Fran.

MS. MAIER: Good afternoon, how is everybody doing? I get about 1,500 emails that are spam a day, so I also get my fair share. Thank you, everybody. Thank you for having us here. I have to say that I have been to a few of the FTC workshops and have found the networking and the post-workshop discussions and some of the things coming out after them to be very valuable, and this is probably one of the most well attended and most participatory of all.

I'm here to discuss TRUSTe and our role in email accreditation, and some of the things that are going on with us, and some of the things that we would like to see go on in the future. First of all, TRUSTe's charter is to build trust between consumers and organizations based on respect for personal information. And so we clearly came to the point that, while webseal privacy is an important issue, email and spam and the potential regulatory actions, the consumer outrage and the business expense and problems with spam really warranted some involvement.

And so we got into this actually starting in 2002, and, you know, our idea and our basic thing was our seal program and what we're doing with the email is try to elevate the responsible players who really do do the right kinds of things.

I want to give credit and thanks to the Lumos Group and the Aspen Institute and the Accountable Net and all of the people who have been working on this like Hans Peter and Margaret Olson and all of these other people, because I think what they did is they helped give us a vocabulary to talk about what's needed and what are the parts of a solution.

And you've heard these over the last few days, so I am not going to spend a whole lot of time, but authentication really I think we've all agreed does not solve the problem in and of itself. Reputation, accreditation and enforcement are other important aspects to it.

And actually, we see authentication as a platform that will ultimately enable the deployment of accreditation and reputation systems, as well as enforcement. And also will aid in the scaleability of solutions.

One of the things that I am not sure everybody is clear on, and this is our take on what some of the differences are between reputation and accreditation. And there are times where accreditation, I think, they're both interdependent and they're both distinct. So, in our view, and I'm sure we could debate this to some degree, reputation is the synthesis of what we know about a sender, their data and a whole range of things about them.

And it works for, I think, very much weeding out the worst spammers and the worst players very quickly, and potentially the data is available on a large range or universe of senders. And I, you know, have to applaud all the reputation programs that are emerging and so on to try and get to this, however new senders will have no history and no reputation. Scheme spammers can potentially find ways of working around that.

I think that's another theme we get is that spammers are almost always going to find a way to try and take advantage and find the holes in any system.

Gray spammers or gray mailers, I think it's a glass half full or half empty, are hard to distinguish with some of the reputation systems, and are likely to especially if the sender is small or relatively new. And a lot of reputation systems are going to be built on algorithms or built on some scoring thing and it's not necessarily going to be clear exactly what is behind it. I doubt if I know exactly what's going on with my credit score. Who knows? Just give me the low range. Okay.

So, when you look at accreditation, really you're accrediting the sender to a set of practices or policies, and hopefully you're going to have some ongoing monitoring about their compliance to those sets of policies and practices. And it should be transparent, you should be able to try to know what you need to do to be accredited. Receivers and senders should both know the rules of accreditation. Gray or new senders can be, I think, more fairly evaluated or more easily evaluated. And hopefully, of course, if you can accredit that they're consistent with best practices and certainly law.

However, the limitations are you're probably not going to be able to do this for everyone, and so therefore large senders are more likely to be joining, especially more formal and certainly more expensive accreditation programs.

TRUSTe's role in this, is we've outlined a strategy to be an independent email trust authority. Basically we want to take advantage of our third party status, our nonprofit status, and become an accreditation resource for legitimate senders and legitimate sender programs.

This involves developing and maintaining email permission and privacy standards, and of course, you know, privacy consent permission standards are something that we know very well. We've been running through the website certification since 1997.

We want to support a legitimate sender program like Bonded Sender and are certainly open to supporting other programs. In fact, what we would like to do is develop an accreditation policy framework where we can take a look at the range of practices and policies that senders will have. For example, their permission level, to opt-in, double opt-in, opt-out. Their time to process unsubscribes, did they take three days, five days, ten days. And, for example, another one might be the level of disclosure at the point of collection. So, we think that this would be a tool for legitimate senders and for receiving networks overall.

With Bonded Sender, we've had I think some great practice and evaluation of this. We think that we have a good set, a solid set of guidelines and practices, and actually I would like to say that it's really easy to create guidelines and rules, but making them into program requirements that you can certify against, that you can check against, that are transparent, is a lot harder, and that takes a lot of work, and I think more work than anybody really understands, but it's essential if you're really going to have a process of certification that works.

The other part of it that I think is interesting is, you have to have guidelines and a process. I think South Regulatory really works, that evolves over time. Because what we might think is a problem now, some spammer is going to come up with some other way and we're going to have to come up with a new program.

For example, websites in 1997 when we had our first set of seal requirements, who could have really foreseen transparent .gifs as an information thing on websites. That, you know, obviously sites are doing now.

Looking forward, we're looking to launch a point of collection seal. This will be a seal that the consumer will see when they're asked to provide their email address and name, and it's going to keep the websites generally to -- well, websites will be the ones using it, to a set of standard regarding their email practices when they collect that name.

We're hoping to expand email accreditation to other sender groups and other kinds of programs, and of course we want to continue to work on this accreditation policy framework.

I'm going to take a few minutes here to talk about Bonded Sender, Craig Taylor from IronPort I'm sure

terms of sharing with third parties or do not want to give an opt-out or I think an opt-in requirement, which Bonded Sender requires. And many of them have overly complicated unsubscribes, and the Bonded Sender standards are fairly strict and don't, you know, those guys get rejected. And I think people forget that even a voluntary program, we have a role in rejecting, and rejecting is almost as important, certainly, as terminating.

Here's sort of a picture of both the email senders and the email receivers that are participating in the Bonded Sender program. And I should have mentioned just earlier that CNET did a case study where they saw that they had a 16 percent increase in their open rates and the case study said that it's a potential shavings of almost a million dollars, meaning the ROI on the program is very positive.

So, we're happy that, you know, and I think many of the companies in here might be testing that and maybe will share their test information as well, since there was a call for that at the last session.

So, when we think about, you know, given that this is authentication and we're talking about beyond authentication, what is it that we want? Well, obviously we want authentication, we want whatever will work, whatever will be adopted, we want you all to just do it. Of course we want the -- it not to be unduly restrictive in terms of intellectual property protections. Sorry.

Most importantly, we want it to be ostensible so that it can accommodate reputation and accreditation. Easily accommodate those things. And the good news is that the specs for both Sender ID and DomainKeys meet this requirement.

I think Ryan Hamlin mentioned earlier today, but we signed onto the letter and the letter with many of the companies who are supportive of Sender ID and DomainKeys is looking at the TRUSTe.org website.

I just want to delve into a little bit more on ostensible authentication record. We believe that basically at this point, you know, you can receive a message, you can check the DNS record for the PRA, you can decide to deliver it or reject. What we would like to see is an additional accreditation check, where you can go in and see, okay, is this a member of Bonded Sender or XYZ legitimate sender program, is it accredited, hopefully by TRUSTe, and hopefully also contain the ability to look at the accreditation accountability framework.

So, what do we think authentication will do for us? Well, Bonded Sender will adopt emerging standards. Right now we do an IP check and right now Bonded Sender is fairly high tech. We actually talk to all of the companies and go through their certification, so we know they are who they say they are. Nonetheless, we think that it would really help and make it more scalable to have a standardized authentication network.

And of course it will help us not only understand who the company is, but set up the platform for accreditation, reputation and other assessment and analysis, and of course ultimately enforcement. We think that with authentication, accreditation will take off and we'll see many of the senders expand, expedentially, I hope, and I think, again, accreditation on top of authentication will elevate practices for the benefit of the consumer so that they are getting permission, they are -- their preferences are being respected, they are consenting to what they're getting, and when they say they don't want to get it, they're not getting it, at least from legitimate senders.

So, that's it for us. Thank you.

MS. DREXLER: Thank you.

(Applause.)

MS. DREXLER: We're going to move on to Craig Taylor, who I think has a little bit to add regarding that. I'm going to ask the rest of our panelists if we can try to keep it fairly brief so that we will have time for question and answers, that would be great.

MR. TAYLOR: Thanks, Sheryl. First of all, I know everybody is thanking basically the FTC and NIST for putting this on, but I actually want to thank all of you people who have actually stayed here the whole time.

So, here is my promise, I am going to try to power through this in five minutes, okay, and so I am going to zoom through this stuff but you guys can hold me to this five minutes, or maybe give me like 30 seconds more, but my goal here is to really push through that stuff.

So, with that said, if I'm going too fast, because I'm just going to kind of go (inaudible). If I'm going too fast, raise your hand or something just to slow me down a little bit. So, but I'm going to get through in five minutes.

So, with that, let me just say it's a pleasure to be here. What I want to do is briefly talk about IronPort's approach to reputation and I want to talk about what makes up a good reputation system and I want to try to put reputation in a context so you can kind of understand how all this stuff fits together.

So, IronPort, in case you don't know, we build appliances. Our purpose built appliance is a high-speed MTA that supports best of breed solutions, including content filtering, virus and spam scanning, and our newly released virus outbreak filters. But for today's discussion, I just want to focus on SenderBase and our second generation reputation filters.

So, with the repu -- basically with an appliance, as a place to stand, if you will, can we metaphorically move the Earth. So, that's the question that I am going to try to answer. Can we use reputation as a lever to fundamentally change the way we manage email traffic?

So, if you look at most mail gateways today, they filter using whitelist or blacklist or a combination of both. Now, this implies either trust, absolute trust, or absolute distrust. Neither of which is very realistic. I mean, if you think about it, if there's generally more trustworthy people and there's less trustworthy people and then there's a lot of gray in between.

incorporates better or worse reputation. So, rather than good and bad, we just have a continuum, which is a score that goes from good to bad.

So, we can use reputation as a measure to incorporate these shades of gray, and a good analogy is applying for a credit card. If you apply for a credit single source from affecting your reputation.

Accuracy: Reputation is fluid, it's changing, there's a lot of things going on in the Internet, there's a lot of things that change in a sender's behavior, so you basically have to be able to compute in near realtime what somebody's reputation is to keep it accurate.

And finally, objectivity. The scoring has to be objective, i.e., it has to be noneditorial and it has to be transparent. You need to be able to see the various data sources to understand how they rate you.

So, with these principles in mind, this is what we used to build SenderBase. So this is SenderBase. SenderBase is our lever to fundamentally change the way we view email. SenderBase collects data from more than that's coming into this database from every continent on the Earth.

So, SenderBase technology is pretty sophisticated, but the result is simple and powerful. If this eco system that we call email is going to function, the inbound load has got to be controlled, not filtered. Participating in an ever-escalating war of more spam and more filtering, which require more and more resources to basically to sustain, just isn't reasonable. It's just not a reasonable model.

Reputation is a very powerful way to get at this. So, a couple of quick customer examples. At Dell, they get 26 million messages a day. With reputation filters, they filter out 19 million messages. They block them. And of the remaining seven million, they basically do rate limiting, and then traditional filters. At the NIH they block 50 percent of the incoming traffic and they limit the rest using reputation filters.

So, basically reputation allows appropriate actions to be taken. Obvious bad mail could be dropped, good mail can be afforded more privilege, and gray mail basically gets rate limited. So, ideally, unwanted mail would never get in the global network at all.

So, our second generation reputation filters are powerful enough to stop unwanted mail at the source. By applying reputation filters when the messages enter the network, typically at the ISP, there's an opportunity to significantly limit the traffic, and thereby reducing the impact on the Internet and basically everybody that's involved.

So, the key take-away that I want you to sort of leave this meeting with is that reputation systems create a feedback mechanism. The feedback allows us to control the load, limit spammers and enforce accountability.

So, when I look at this, I really see a bright future. You know, we've got new authentication standards on the horizon, when you combine those with reputation filters, we really do have the opportunity to change the way we manage mail.

If you want any more info, you can check out our website, and how did I do with my five minutes? Six, all right, well I gave you an extra minute. Thank you very much, it's been a pleasure.

(Applause.)

MS. DREXLER: Thanks. Now I'm going to move on to Des Cahill, and again, if I could ask you all to try and keep it brief so that we have some time for questions and audience participation.

MR. CAHILL: I will try to keep it brief. And while I'm getting this started, in the interest of time, I want to say thank you to the FTC and NIST, and all of you, and especially to Sheryl for putting together this panel.

And my observation leaving yesterday was I was a bit discouraged hearing all of the debate about the multiple authentication standards and I was feeling slightly discouraged that we wouldn't get to a point where all those authentication standards could be really implemented in the real world, but after an incident today, I'm heartened, because I have an example of where multiple authentication standards can be supported in the real world.

I was coming in today with several of my colleagues and we were going through the authentication process as we were entering the building, and as I was fumbling to remove my cell phone and my glasses and my keys and my change and my badge and throw them in, and I was asked for my driver's license and I got out my driver's license and I got in. And then my next colleague also got out his driver's license and got in, and my third colleague didn't have his driver's license, but he had his Costco membership card and it had his picture on it. So, he was able to get in. So, I just

So, I think of accreditation and reputation as killer applications that rest on top of the platform of authentication. And I think it's great there's so much debate and passion around getting unification around authentication and getting something out there in the market.

So, authentication is about I can tell who sent me this mail. You don't know if that's mail that you want, but you know who sent it so you can hold them accountable.

Accreditation is what we do today. This emailer has verified good emailing practices, and I think Craig did a great job of talking about reputation. It's data, multiple forms of data that exist that say, this is wanted email by most recipients, so I can make a judgment about it.

I see accreditation and reputation as two sides these up here. This is how the real world defines it.

First of all, it's obvious, I'll restate the obvious, authentication is necessary. We are recommending, or actually we will be requiring that our customers adopt SPF Classic. We will be encouraging our customers to publish Sender ID records as well. And I think the bottom line message here, and when we work with senders, is that if an ISP says that they need to jump up and down and bark, they will jump up and down and bark, but that means that they are not going to be treated like a spammer.

So, what I'm saying here is I think it's upon ISPs to accelerate their testing. I think it's upon the technical community within the email world to work together and get some authentication standards out there. Fast. Because senders want this. Okay? This is a very inefficient process we're going through right now. And if it's not right, we can fix it later.

But authentication, again, is the operating system with a platform. You know, spammers first to adopt SPF, legitimate companies to send spam to. You are who you say you are, that doesn't mean I want your mail. So, that leads you to once you have authentication, accountability.

So, can I predict the quality of email based on known certified practices? Within Habeas, our accreditation process is about looking at sender practices at a domain level, a company level, are they a real company, can you physically reach them, in their domain. Their own mail may be fine, but do they encourage affiliates to send out spam email on their behalf, and then at a mail stream level, which they would do at an IP level.

And then we publish that information in multiple ways. That accreditation information. We publish it within a -- think of it as a meta, metadata within the header, within the X header. We publish it via DNS, in regular DNS flavor or coded DNS response, and we also publish it -- will publish it in HDDT as well, so that there's a profile of information or a corpus of information about the senders, and that would be the Habeas corpus. Sorry, bad pun.

And then, a very important part of the accreditation is compliance monitoring to make sure thpart of the transparency by collecting a large set of information about sender practices that allow receivers to make a more informed decision about how to treat that mail. And what we believe that drives in turn is we -- that drives some transparency and commonality among ISPs on their treatment of senders, and it drives senders towards best practices.

Reputation: Objective data about the actual behavior of the mailer. Craig talked about a lot of different data points that IronPort uses. Fran talked as well about some of the characteristics. Its a database, so it scales well. Unfortunately, though, there's typically not usable feedback that's going to the sender.

We fundamentally believe that companies, whether they're gray companies or they're good senders that occasionally make a mistake in their sending, that they want usable feedback. That's what we hear from the senders that we deal with. They want to be legitimate members of the email community. And reputation systems are great for prefiltering at the edge of the network and dropping, you know, 17 million emails a day for Dell, but you've really got to take legitimate companies that are being dinged in their deliverability, there needs to be a way to get information back to them about

And then I would echo comments that were made yesterday that authentication needs to be more granular than domain level. It needs to address the needs of small and medium business. It needs to scale to address the entire community. However, having said that, I think it's -- we need to get something done quickly. If we can only address the needs of a certain class of mailers, better to get that going now, get that happening, learn, get experience, and then bring it to the rest of the eco system.

Thank you very much.

MS. DREXLER: Thank you. Now we are going to quickly hear from Tonny. And just so the remaining panelists know, we only have about ten or 15 minutes

1 It n4Dn the entire communioREXLER: Thank you. NtFr6.0000000 ry00 1.0

cfhear frof 13t's 2.00 0.0lrbring it to

Email authentication does help, but a critical component that still is necessary is statistics-based reputation, and what I would like to talk about today to share with you is what is statistics-based reputation and how does it work.

But first a little bit about Mailshell. Our antispam library is licensed by over a dozen OEMs around the world. It's used by over 4,000 companies, and ten million consumers worldwide. There are four engines in our antispam engine that checks over or applies over a million checks.

The one that I would like to focus on is the spam repute engine that applies the statistics-based rules to compute the reputation of a message. I define reputation of an attribute as the difference between the number of spam versus the number of legit for that attribute. What I call the spam repute index. For example, the reputation of an IP address is the difference between the number of spam from that IP address versus the number of legit from that IP address.

We track the reputation of hard to fake attributes, such as every IP address, every domain, every sender fingerprint and every message fingerprint. To fine tune the results, we also track the reputation of related attributes, such as country of origin of IP, the domain owner, domain server, domain registrar and also accreditation services.

The results of a reputation system are only as good as the data that goes into it. We collect data from our global network, which includes millions of users of our products, and the global data centers that search the world for spam servers. Zombies and spam messages. And cooperative partners that share data with us.

What is the -- how do we use the Mailshell spam index in practice? When we get a new message, we first extract the spam attributes from that message. If these spam attributes are spoofed, then we just throw the message away. If we're confident that it's spoofed. Second is we compute the spam repute index for every attribute, and then third is we compute the overall spam repute index for the message by combining statistically the individual attribute scores.

The impact of spam repute, we found that the spam repute is very accurate, just alone. It is also the most effective weapon against the growing phishing problem, which I believe is the future of spam. And it's being employed now, with very little cost to email senders and receivers.

How to improve? The key to improving is

authenticating and preventing spoofing of all the rightful owners of not just the sender, but of IP addresses, domains, and the message content itself. What we're looking for is more sources of data, more cooperation, and we're hoping help from the senders, reputable senders as well, to keep their reputation high.

Thank you.

(Applause.)

MS. DREXLER: Thanks for keeping it brief, Tonny, and now we're going to move on to Richard.

MR. GINGRAS: No time for slides, no time for jokes, no time to thank the FTC. Goodmail Systems -- don't laugh. Goodmail Systems was founded about a year and a half ago and we've been working over that period of time very closely with very large ISPs, and very closely with members of the email service -- email marketing service companies, like the ESP Coalition, Hans Peter Brondmo, one of the authors of the Lumos papers is on our board of advisors.

We spent a tremendous amount of time over that period thinking about how to develop the appropriate accountability platforms that clearly I think everyone feels that now has to be brought to bear on the problem of spam.

The accountability platform that we have architected is what we called Trusted Class Email. So, let's talk a bit about that. First of all, you know, the value of any communications medium is tied to its reliability. And I think if there's been any great loss in the last several years, it's that loss of sense of reliability and trust in email as we know it. It's been fueled with maybes instead, right?

Maybe that message that I'm expecting to receive from United Airlines with my itinerary will get to me, maybe it won't. Maybe the message I sent to mom will get to her, maybe it won't. Maybe that message is from Citibank, maybe it's really not, just looks like it. Maybe that domain authenticates properly, but maybe it's still spam. Maybe my message will be received properly by ISP A, but it won't be received properly by ISP B.

These are not the characteristics of a reliable communications medium. And whereas I very much agree with the fellow from IronPort about the gray scale of sending behavior out there, we will have failed as an industry if we cannot create the systems that assure delivery of permission-based messages from certified senders.

We will have failed. These are legitimate entities who have legitimate reasons to be using email for large volume sending purposes, profit, nonprofit, large and small.

So, let's talk a bit further. We've been doing a lot of research with consumers over the last year, and there are two things that really popped out to us in terms of their desires. One was I want a conveyance of certification of legitimacy. Help me be comfortable that this message is real. And those numbers have shot through the roof, not surprisingly, over the last several months with the onset of the greater visibility of the phishing problem.

Secondly is they want that sense of assured delivery. And of course so do senders. Assured delivery, a conveyance of certification of legitimacy. The question is how do we get there? And I can tell you that accountability platforms are difficult, reputation systems are difficult. There's a lot of rigor that needs to be applied to this if we're going to pull it off effectively.

One of our objectives, by the way, in creating this platform, was that it be all-embracing. I took very much to heart the comment by a speaker this morning, Dawn Rivers-Baker, about the fact that this should not be a system that is simply for the folks who are in the know. This is not for the hundred folks who know who to call.

When we look at the data, we see that there is easily well over 100,000 legitimate entities in the United States, probably two or three times that, who use email for volume sending purposes today. And every one of them deserves the opportunity to participate in systems that allow them the same benefits that we're talking about here.

So, when we think about accountability, what do we think of? There are five key points in our approach to it. One is identity, and that very rigorous approach to identity. And we're not talking about domains, we're talking about entities. We want to know who they are. We want to know if they've been in business longer than a year. We want to know how many employees they have and does that verify out.

So, everything we can do to create a very strong contractual path of accountability to that sender. Absolutely crucial that we do that. And again, do it in a scalable fashion. Needless to say, not showing up at the website with a credit card won't cut it.

Feedback mechanisms from the user. A big part of our system is that we have a tight closed loop feedback system. The messages are labeled in the inbox in the interface for the nonspoofable and there's a feedback mechanism there so that the user can unsubscribe reliably or complain if they feel the sending behavior is inappropriate. Maybe they don't agree that the person has the permission to send that message.

That feeds into a reputation system. And if there's one thing that we learned about reputation systems, it's that if we expect senders to be held accountable, it's only fair that we do hold them accountable in a fair and transparent fashion.

You know, as I've worked with the likes of Dave Lewis or Margaret Olson, what they have said is we understand the need for our behavior to be monitored and held accountable, but do it fairly. I don't agree with mixing up reputation data from rogue blacklists who themselves aren't accountable for their behavior. So we need tight closed loop systems such that the feedback on a message is tied to that specific message. Therefore as a result we get very, very accurate data about their behavior.

Each one of our messages is tokenized and signed so that we know exactly how many messages were sent by that sender via trusted class email, we have the right denominator against the complaint levels, we can have accurate reputation measures so that we can reasonably, in their eyes as well as ours, enforce our policies.

And enforcement obviously is the fourth element. There need to be penalties if people go out of line. If they go way out of line, they're kicked out of the system. It's that adjustment in their fees, it's that adjustment in their privileges. If you have a tokenized system, you can actually adjust the quotas applied to a sender if their behavior is not up to snuff.

Also when you have a tokenized system and you have a closed loop feedback system, we have near realtime data coming back. So that to the extent that we see a rogue spike in behavior, maybe because somebody's system was hacked into, we can deal with that within hours, within minutes, if necessary, so that no further messages get sent at least as trusted class messages out of that entity.

And the last is we do feel there needs to be a degree of economics applied to the system. For a number of reasons. One, because these systems are expensive to build and operate. Another to motivate list hygiene, to motivate sensible sending behavior.

I won't forget the comment from someone in the direct marketing industry, who I won't name, but a notable person who said, "we can cite all the good principles of sending behavior we want, but I can tell you, Richard, unless there is financial friction in the system, there is no motivation for us to do the right things with regard to list hygiene and volume sending behavior."

Why are we sending two messages a week when maybe actually it would be better to send one every two weeks. Motivate those activities, and also for that matter share the ballooning cost of email hygiene that right now is entirely borne by the ISP. And that's significant. The messaging entities of this working group says that $8 to $12 per mailbox per year, and that's starting to hit consumer costs.

So, either we find ways for the volume of senders who benefit from the medium to participate in those costs or we're basically saying stick it to Joe consumer, we don't think.0000 cmgpcmgpcmgpgllooning cost of emaila that kind of accountability platform with that degree of rigor such that we can accurately and fairly and transparently allow legitimate senders to benefit from assured delivery and at the same time hold them accountable for their behavior. Thank you very much.

(Applause.)

MS. DREXLER: Meng Weng Wong?

MR. WONG: Thank you, Sheryl. How much time do we have?

MS. DREXLER: Well, we're running pretty low, so I think if we want to leave time for a question or two, then we probably have about five minutes.

MR. WONG: All right. Well, with five minutes.

MS. DREXLER: Well, you have five and we need -- we have Hans Peter at the end.

MR. WONG: Right. Okay, well, instead of doing a full PowerPoint presentation, maybe I'll just do a couple of screen shots. And I can discuss -- okay, so here's what I've been working on for the last couple of months. This is not that different from what we've already seen. Can you guys all see this? It looks awful. Sorry.

Anyway, this is a sample webmail inbox, all right, and you're going to have just your usual mail. On the left there are some smiley faces, and that's when mail comes in, it authenticates and it doesn't have to authenticate using SPF or whatever, it can authenticate using DomainKeys, we haven't written that yet, but we plan to. And it also is from a known good sender.

So, I sent myself mail from Gmail and from Hotmail and that's why I got a green smiley face. If it came from a forged address, there is Amazon and eBay publish SPF records and so there is a forgery failure on those, you get a red frowny face. And, you know, there are different categories based on what the authentication versus reputation status is and sometimes you just get a face.

The idea is that I think in the future we will have different folders, right? We have -- like today we have the regular inbox and we have a junk folder. I think in the future it will be really nice to have a not junk folder and all of the things with the green smiley faces could just get foldered into that by default. And I would wake up in the morning and go to my not junk folder before going to my regular inbox. I think that would be a really nice feature.

So, you know, this is one of the things that I wanted to show you. Let me show you the other thing real quick. Here's my other really awful looking screen shot. I'm sorry. That's barely even legible.

What we have here is a reputation and accreditation aggregation system. I think a lot of these fine people are going to come up with fantastic reputation schemes in the future, they are going to have all kinds of really clever ways to tell when someone is good or bad. What I've put together is a way to, instead of having to query, you know, all 12 of them, you could query one place and get back 12 results, which is just a little technical optimization, but I think it will be worth using as we move into the future. Just so you don't have to choose what to use all the time.

If you've ever been to the website RottenTomatoes.com, you know what I'm talking about. And if you haven't, you should check it out, it's really cool.

I don't have very much time to talk more about these. I will actually be talking more about them next week at the Inbox event, inboxevent.com, on Tuesday, which is actually the day before Inbox. You're all invited to come and hang out, if you want to come. You can mail me for more details.

So, instead of speaking for a half hour, I just wrote down everything that I have to say, and I have this white paper here. There was a big stack of them outside. You can either take the full version, which is really thick, or you can just take the cover page which has the URL for the full version on it. So, depending on whether you're flying home or walking home or whatever, take whichever one you want. Well, anyway, that's all I have to say. Thank you everyone. Hans Peter Brondmo is next.

MR. BRONDMO: I am not going to get up just to save you some time.

MS. DREXLER: That's great.

(Applause.)

MR. BRONDMO: So, I think much of what needs to be said has been said, so I will try to make my remarks very brief, and I just want to touch on and highlight a few things that I think are important as we look to the future. I think the -- you know, a lot of big fancy words have been thrown around, accountability has been mentioned a lot, transparency has been mentioned. You we have authenticated mail, now what?

Well, this all started with a question about accountability -- that related back to accountability. How do we hold these guys accountable? How do we stop guessing who the spammers are and step back and say we want to identify people based on behavior, based on history, et cetera.

And accountability has two components. Surely one component is you need to know who they are. And not only do you need to know who they are at the moment, you need to know who they are over time. So, authentication and persistence are two very important components, right? If you only saw me for the first time today, I have no reputation. If you've seen me for six months, it's starting to help.

But the other piece, which we've heard mentioned a few times and which I think is very, very important here is captured in the word transparency. Because once, again, assuming we have authentication, you just got an email from my personal domain, HansPeter@Brondmo.com just sent you an email. If you're -- say you're Yahoo! and you got my email. Well, if I'm a spammer and I'm sending from that domain and that domain has been authenticated, all you know is it came from brondmo.com, you don't know anything else, right? So the mail came from brondmo.com, you've just received it, it's the first email you've ever seen. If you're a small player, you do not know what to do beyond that. Authentication is not going to help you one bit.

If you're a big player, if you're AOL or Yahoo! or Microsoft. For me to send email to Yahoo! or Microsoft or AOL and make them an economically proposition, whether I'm a phisher trying to steal information or a spammer trying to sell you Vicodin, I have to do that scaled.

And so Yahoo! will very quickly see a lot of email coming from this authenticated brondmo.com domain and shut me down. They have information, they have their own information. They have their own transparency because they get so much mail.

Now, if you're a small domain. If you're I like to think of it as the other 50 percent, the fifty percent of domains out there and traffic that does not belong in this small collection of large ISPs, you will have no idea what to do. So, that's where all the stuff we've been hearing about today comes into play.

But what it really is all about is transparency. I need to be able to look and see what the behavior is. And so I have a very basic call that I would like to make, and a request to the big ISPs, and the big players in the space, which is share your information.

The real challenge here is getting access to the information about what senders are doing. Because if we don't share that information, if we don't get access to the information in the network. This is an information problem. And if we don't get access to the information about what people are doing, authentication won't matter for the other 50 percent. Because authentication won't tell you anything about whether it's good, bad or ugly. It will just tell you that it came from the domain that sent it, but nothing else.

So, you need the kind of stuff that Fran talked about, and what TRUSTe is doing with accreditation. I actually happen to disagree that accreditation and reputation is the same thing. I think they're different, and I won't get into the details of that because it's a little complex and it's late in the day and you haven't had the chocolate that I just managed to steal on my way in.

But there is a subtle but important difference there. Regardless, you need accreditation. I need somewhere where I can basically step up and put my credentials and have my credentials on file. So that what I'm sending in if I haven't developed a reputation, someone can go to that trusted entity and say is this guy known or not.

But then the reputation piece is really the objective measure. It's the credit score if you like. It's that information that gets collected in the network. And the information that gets collected is the valuable thing here. And my concern is that we limit the viability, the overall viability of the network by not making that information widely available.

So, that [illegible]

say.

MS. DREXLER: Thank you very much.

(Applause.)

MS. DREXLER: And I think what we're going to do is, unfortunately and ironically due to some technical difficulties in accessing the Internet before we started this panel, we are not really going to have time for questions and answers, but I encourage you to come seek out our panelists afterwards if you have any specific questions. I think we have a quick announcement first before we hear some closing remarks.

MR. SALSBURG: Thanks. As you all know, putting on a conference like this requires a tremendous amount of work, so before we introduce our final speaker, I want to thank those people who really made this conference reality. First, from NIST, Donna Dodson and Bill Burr, we really thank you for your work in helping us understand the concepts that are involved and 1 soskRhLesf

12 bgood

driver's licenses and Costco cards when people came in. These include Justin Krypel, Rebecca Hughes, Heather Thomas, Leah Weiss, Josh Ferrentino, Zack Mabel and Greg Dworkowitz.

Another special thanks to our Office of Consumer Business Education, people who you didn't see here, but whose notepaper you wrote on, whose logo for the summit you admired, and these include Callie Ward and Carolyn Riley and Jonathan Morgan, they have a way of making those of us that work in the operating divisions of the FTC's Bureau of Consumer Protection always look professional. So, thanks to them.

of working with four of the best colleagues who dug right into the subject matter, who are generalists by nature, that's what we're trained to be, but when it comes to technical issues, they mastered them, they helped make our questions sharp and helped make it so that we could really raise the level of discourse of this conference.

A special thanks to Sana Coleman, to Sheryl Drexler, to Colleen Robbins and to Katie Harrington-McBride. Thank you all.

(Applause.)

MS. DREXLER: Okay. Well, I want to thank all of our panelists in the final panel, and thank you, Dan, for that. I want to thank everyone for sticking around until the end of this really productive Summit.

And now we're going to hear some closing remarks from Commissioner Orson Swindle, who was sworn in as a Commissioner on December 18th, 1997. He has played a key role in putting spam on the front and center of the FTC's agenda, and so Commissioner Swindle, we thank you for being here, we look forward to hearing from you, and now I'm pleased to introduce to you Commissioner Orson Swindle.

COMMISSIONER SWINDLE: Thank you very much, Sheryl. I have several pages of remarks here, which will take about 40 minutes, but bear with me. You're the most persistent group of people I've ever seen. You realize that it's going to be pitch black dark when you get out of here, and that's terribly discouraging, at least it is to me.

As you've noticed, I haven't been here, we do have a link with our computer system so we can watch some of this stuff, but I listened to a couple of the first sessions and I decided that I had one of two choices, I could either come in here and in a matter of maybe about two hours be so totally befuddled by what you were saying and talking about that I would be of no use whatsoever, or I could come in here without knowing anything about what you've talked about and give you a pep talk. So, I am taking the option of the latter, because I have no idea what you're talking about, it's way over my head.

Just a quick review of history, and by the way I would like to echo Dan's comments about the staff that worked on it, the folks over at NIST that worked with us and others. It's an enormous effort to put one of these on, but it would be nothing if we gave a party and nobody came. Thank you for staying here this long. This has got to have been a real challenge to sit through all this, and we have high level lobbyists and people like that sitting around here and keeping tabs on everything. But it's great to see you and see you still awake at this particular point in time.

Just a quick review of history, the spam issue, Sheryl was saying, it's sort of been on my mind for several years. About three years ago Tim Muris and I called in all the ISPs, or at least a number of them, not all of them obviously, and some of the big guys and we said hey, guys, we don't want any advice from you, for God's sake solve the spam problem, because we're killing the killer app out here. If we don't get this solved, we're going to turn off a hundred gazillion consumers, and if we do that we're going to kill off the system or at least certainly put a lot of impediments in the way of it.

And we were dealing with a complex problem. Spam it was mainly at that point in time, it was a nuisance, it was sort of a novelty to some and even got sort of nasty, but we had a workshop following that little session and prayer meeting and we had several more prayer meetings with this same group and said, what are you doing, what are you doing, are you getting it done?

And we had the workshop, and the workshop was fascinating. It was filled with enthusiasm, it was informative, it was emotional and in some cases combative. And since then we've seen, in my estimation, at least, a tremendous amount of progress in helping consumers deal with spam. But we all know, spam is 80 percent of all email now instead of 50 percent or whatever those huge numbers are, but when I talked at the spam conference last year, I said it seems to me we have two concerns here. I call them spheres.

We've got the consumer sphere and I said for God's sake, empower consumers to deal with this at home, because they're getting turned off and they're going to get turned off real quickly, and that's the emotional sphere. And then there's this big ogre over here that's sitting above all the ISPs and all the technology and all the systems and all the networks, and that's the technical sphere, and I said we've really got to work on that.

But we see a lot of progress and the empowering consumers, now we've got to deal with the big ogre. And this is nothing more than a continuation of the spam problem but addressing the technical aspects of this, but we've got to solve it. We're here today, the FTC, and all of our friends in government, confessing to you that we don't have all the answers. We don't even understand the questions sometimes.

You're the brilliant people, you own 85 percent of the Internet and all the information technology structure that exists in the whole world, and you caused this, so it's your problem to fix.

No, but seriously, we're here to listen and learn from you, and to work with you, and express to you our belief that we can all get to the bottom of this. We will never solve it completely, there is no answer, and you know that better than I. I just, I'm just fascinated by the few presentations that I did hear, how smart you folks are. But it's going to take all of us working together and in our different capacities to find the answers. We can hold the forums, but the private sector has got to solve the problem. I'm totally convinced the private sector has got to solve it. We can help, and we will help, and we're standing by to help, but please continue to educate us, because we need to learn a lot.

If you don't solve it? Guess what? The guys up here on the Hill will feel that they've got to do something, and they will try to solve it, and if there's anybody in here who thinks that's the way to go about this, meet me outside and we'll talk about it in the dark, but I really don't think that's the adequate way to address this, but the one thing that we all agree to, or we should, we've got to solve the problem. Not solving it, delaying in solving it, dragging it out, having -- I was about to say petty competition based around proprietary interests and the business model that we own and they own, that's legitimate. I mean, we all understand that.

But there comes a time, I think, when we have to do things for the common good. And I think in my simple definition of what standards are, standards are aimed at trying to do something for the common good, because there's too many ways to do it, let's see if we can come up with a good way, or ways, it doesn't have to be just one, and we all have to work together to do that.

There are legitimate ways that we can do that, but again, you guys, you own it all, you've got to come to the table. There are ways we can do that without running into antitrust suits and things like that that we might be inclined to file if we don't hear the right answers, but we've all got to work on this.

So, bottom line, my summary is not a summary of what you've been doing, I'm just trying to finish this up within three minutes so you can go home, but I urge you all here to leave here knowing that we're prepared to work with you, we've got great staff. We Commissioners don't know anything about this stuff. We believe what the staff says 90 percent of the time. Occasionally I challenge them, but we do learn. We learn slowly, but see, as you have learned, and are teaching us, our staff is learning and becoming experts and they will convey that as much as we can tolerate to us and we'll all work together with you to try to solve these problems.

This problem is technology and innovation. It's not regulation, it's not new laws, but through the technology and innovation, you can help us in our law enforcement role. If we can arrive at some reasonable standards that we can all share, we can all develop and we can all agree upon, that alone will help us start identifying spammers, and that would be a huge step forward, because right now, as you know, that's a tough one. If we can't get to them, it's going to be sort of hard, you know, we can only file so many John Doe suits I guess. We've still got to find somebody to do something to them.

So, this technology will help filter out and reduce the problem substantially, I suspect, as someone said, it's not a perfect solution, all of this has been discussed at least since I've been in here for the last 30 or 40 minutes, it's just absolutely great stuff.

The point being there is no simple one path to solution, but all of it has got to be played, we've got to all be talking to each other, we've got to all seek a common good solution, and I think if we do that, we're going to make a difference, we'll start diminishing the amount of spam. We may not diminish it, but nobody will ever see it, we'll just do away with it. We're going to start finding the people who are doing it, that will start to really diminish things when people start going to jail or paying heavy fines.

So, we've got to work together. Doing nothing or dragging our feet, or playing games is not an alternative. It's absolutely not an option. We have to solve the problem. We have to get this done.

And I read an article in I guess the Washington Post yesterday and it's a rather expected and gloomy expectation of John Levine and I don't know John. John, are you in the room? John is not in the room, but in the Washington Post concerning domain-level authentication. Let's gather again next year about this time, preferably let's do it a little earlier so we can go home in the daylight.

Let's gather again next year just like we did a year ago, we did this year, gather together next year having made a great deal of progress. We won't find the ultimate solution because some of you heard me say, this

CERTIFICATION OF REPORTER

DOCKET/FILE NUMBER: P044411

CASE TITLE: EMAIL AUTHENTICATION SUMMIT

DATE: NOVEMBER 10, 2004

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

DATED: 11/29/04

SALLY JO BOWLING

CERTIFICATION OF PROOFREADER

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

DIANE QUADE