FEDERAL TRADE COMMISSION

I N D E X

P R O C E E D I N G S

- - - - -

WELCOME

MS. DREXLER: Good morning, everyone. My name is Sheryl Drexler. Welcome back to our second day and final day of the Spam Summit: Next Generation of Threats and Solutions. Before we get underway, I just have a few brief housekeeping announcements I'd like to make, so bear with us.

First, if you have a cell phone or anything else that makes noise, please shut it off now. In addition, this is a government building. So, we just wanted to inform you that in the unlikely event that we have an emergency, there are exits both the way you came out as well as in the back of the hallway that you entered through, and there is a remote possibility we will have to do something we call shelter-in-place, and in that case, we will go right out into the main hall, back in the back there, the main galley-way.

So, audience participation is key, so we do ask that you please ask questions. We will also have roving microphones at the end of the panel for the question and answers. We do ask that you wait for the microphone and make sure that you speak your name clearly and your affiliation. We also do have question cards in your

folders, and there's additional ones available out in the front, and someone will be around to collect those.

And we also invite our webcast listeners to send an email to spamsummit@ftc.gov, and we also wanted to let you know we do have a wireless hot spot here, and the code in order to use that -- there are brochures out in the front, and additionally, I'll tell it to you now. It is BACE071107, so feel free to use that as well.

I wanted to let you know, a little lost and found item, we had a pair of glasses left here yesterday. So, if they're yours, please come claim them.

And it's now my pleasure to introduce to you Lois Greisman, who's the Associate Director of the Division of Marketing Practices in the Bureau of Consumer Protection, and she is going to kick off our first panel. Thanks.

DETERRING MALICIOUS SPAMMERS AND CYBERCRIMINALS

MS. GREISMAN: Thank you, Sheryl. Good morning, everyone. Welcome to day two of the Spam Summit. I'm delighted to be here, particularly, moderating this impressive panel.

I was -- a couple of opening remarks. I actually was not here for the program in 2003, and what is clear, though, based on my knowledge of that and what I heard yesterday and what I anticipate we'll hear today, the times they are a changing. This is quite dramatic. There's been some discussion of spam as a nuisance, but by and large, it is spam as a cyber-crime. It has made a major transition.

And what also became clear yesterday is that there's a robust competition in the malware economy. You can rent a bot for $300 to $700. You can buy a spyware kit for as little as $17. Phishing toolkits are down from about $1,000 a year ago to perhaps $100 these days.

Chairman Majoras, when she spoke yesterday, emphasized the FTC's civil law enforcement role in combating spam over the last several years, having brought nearly 90 cases, roughly two dozen under the CAN-SPAM Act. But really, what we heard a lot of yesterday is the challenge for criminal law enforcement,

Property Section, known as CCIPS, where she prosecutes a variety of computer crimes. Also, in the interest of full disclosure, I must say that she previously worked at the FTC, having left here just about a half year ago.

Next to her is Aaron Kornblum, who serves as senior attorney on Microsoft's Internet Safety and Enforcement Group, and he has taken the lead in Microsoft's global enforcement activities involving spam and phishing.

Next to him is Keith Mularski. He's a special agent with the FBI who works with Tom Grasso and takes a lead role in the National Cyber Forensics and Training Alliance in Pittsburgh, helping to track and prosecute some of the most significant cyber-threats.

Next to him is Robert Shaw. He heads the International Telecommunication Union's Development Sector's ICT Applications and Cyber-Security Division -- that's a mouthful -- and serves as the point-person assisting developing countries on cyber-security and spam issues, and he joins us from Geneva.

Last, but hardly least, next to him is Hugh Stevenson, Deputy Director in the FTC's Office of International Affairs. He currently heads the U.S. delegation to the Committee on Consumer Policy at the OECD.

And without further adieu, let me turn it over to Gene.

MR. FISHEL: Thank you very much, Lois, and good morning, everyone. It's a pleasure to be here this morning. Again, I'm Gene Fishel. I'm a prosecutor and chief of our Computer Crimes Section at the Virginia Attorney General's Office. Basically, in my brief five-ten minutes this morning, I am going to talk to you a little bit about a case we prosecuted a little over two years ago and kind of give you the perspective from the state side of law enforcement and the challenges we face in prosecuting spam cases and some of the issues we're facing now, mostly legal issues, with this case, because this case is on appeal, going through our state courts, and ultimately might reach the United States Supreme Court, but -- and if we -- I have some slides here.

In Virginia, we are uniquely situated. We have a lot of Internet traffic that flows through our state, and so that allows us to pass laws that may have more of an effect than maybe some other states, because what with all the Internet traffic that we have going through Northern Virginia, being a very high-tech corridor, this allows us to get jurisdiction over certain people, and you are going to see in this case I am going to discuss

that jurisdiction is a key issue. So, it allows us to pass some laws that may have more of a punch than other states, but this is why the jurisdictional issues -- this is why federal laws are so important. I think you'll see that at the end of this.

In 2003, we passed a criminal felony spam statute in Virginia, and ultimately, that criminal statute served as the model for the criminal portion of the CAN-SPAM Act, which was actually passed later that year. Ours went into effect in July of 2003. The CAN-SPAM Act, I think, went into effect later in 2003.

Of course, one of the reasons we have -- get jurisdiction in criminal cases and have this Internet traffic is because we have AOL headquartered in Virginia, AOL being the largest Internet service provider, it's headquartered in Loudoun County, and, in fact, in the case that we prosecuted, again, a little over two years ago, it seems like forever in this world, because the methods have changed for sending spam. Criminal spammers are using different techniques, and you'll probably see, as I'm just kind of giving you a brief overview, that most of these methods probably aren't used anymore.

I mean, I'm sure some spammers are using them and some other people can probably talk more so on that

than I can, but, you know, two years ago -- we actually detected three years ago with the help of AOL, you know, these were methods that -- that nowadays, the guys are using botnets and zombie networks to send the spam out, and you are going to see this was more of a fraud-type scheme to evade the filters at AOL.

And, again, we worked -- we worked very closely with AOL in Loudoun County to develop this case, and they have a crack team of investigators, one of which you're going to hear from today later on a panel, Margot Romary. She was actually one of our witnesses in this spam case. So, with the help of AOL and Jon Praed, who just walked in late on my talk, who you heard yesterday sitting on a panel, all these guys helped us out tremendously in developing this case.

I prosecuted this case along with two of my colleagues in the office, Rusty McGuire and Lisa Hicks-Thomas, and we prosecuted the defendant in late 2004, and the case was significant because it was the first time someone had been tried and convicted under a spam statute as a felony. And, just to give you a little bit of overview, this case was against a guy named Jeremy Jaynes. He was based outside of Raleigh, North Carolina, in Carey, which is a suburb, a really nice suburb of Raleigh, and you will see how nice it was,

because I am going to show you his houses on this slide.

This guy was, according to Rokso, ranke

you have to be caught sending 12,000 a day, 100,000 in a 30-day period, or a million in a year, and, of course, these -- not only do they have to be unsolicited emails, not only do we have to prove that they're unsolicited emails, they have to be -- the routing and transmission information has to be forged. It has to be fraudulent. And, of course, the reason why they were doing that was to evade the AOL filters so their emails get through and get to the ultimate user.

So, AOL detected thousands and thousands of emails over several days and turned this case over to us, and our investigators in our office had to pick up from there and do the legwork and actually go to see -- you know, go down to the downstream providers, see -- trace the connectivity, trace the money -- which was very important, that led us ultimately to these guys -- and travel down really to Raleigh and dig around to see if the addresses behind these domain names that were being used are real, if the names are real, and that's essentially what we did, and really took up a lot of our time.

We are not the biggest unit in the world, and this -- of course, one of the problems with state enforcement of this is -- as opposed to federal enforcement, who has a ton more resources, is that these

are very resource-intensive cases, and this tied up our unit for months. It tied up our unit investigating this for six to eight months, maybe, trying to develop this case to bring it to fruition.

But you can see here, this is Jeremy Jaynes right here. You can see the progression, what he looked like prior to his indictment in December 2003, he was a happy-go-lucky guy. We estimated his worth, at least that we knew of, at about $22 million, I think. He was really making a lot of money doing this, and that's just what we know of. We figured there were offshore accounts and all sorts of things that we couldn't get our hands on as state law enforcement. Fortunately, we had the help of federal enforcement.

You can see, December 2003, that middle picture is actually the morning we kicked open his door at 5:00 in the morning of his house and walked in on him, and he doesn't look too happy, and, of course, December '04 is when he was -- after he was convicted and locked up.

But, of course, you know, there -- as everyone knows here, there are several victims. There are not only the victims who are the people who are falling for his fraudulent schemes, which the actual content in these emails was fraudulent. He was selling bogus products, penny stocks and Internet history erasers that

never showed up and all this stuff. But also, of course, AOL and the other Internet service providers have to process this, and it costs them millions of dollars, and that's the point we had to get across from the jury.

Of course, he was reaping millions of dollars. In the upper left of this screen, it was actually a really nice residential neighborhood. This was his office. He didn't have really any furniture in this house. He was just using it as a spam operation out of the attic of the house, and in the lower right, that's actually his residence, which was a really nice multimillion dollar mansion outside of -- again, in Carey, North Carolina.

But the office up in the upper left-hand corner is where we actually barged in on him at 5:00 in the morning that December morning of 2003 and actually caught him in the act of sending 5 million spam emails. We actually took screen shots, walked up there, and he actually had his operation in -- in the attic of the house.

And when the investigators -- when the officers walked in there, we had cooperation with federal law enforcement down in Raleigh, they found cases and cases of hundred dollar bottles of wine, 12 in each case, and

the night before these guys apparently have so much money that they were drinking the wine out of wine glasses, throwing the wine glasses away, not washing them, and then grabbing a new wine glass to drink more wine. So, these guys were living the high life.

But this is his attic. He had -- this is where he was actually sending his spam. He had, coming out of that attic, 16 T1 lines coming out of the attic. So, the Attorney General's Office, where we have, like, 300 employees, we have T1 lines. He had 16 T1 lines, and the neighborhood actually wondered why the phone company kept coming over there and installing new lines. They thought it kind of odd. But this guy had 16 T1 lines. He was spending tens of thousands of dollars a month on Internet connectivity to get out of there, to get his -- to pump his spam out of there.

So, anyway, this thing went to trial. It ended up being a two-week trial. We had to do a lot of legwork, and as I mentioned earlier, our investigators found that the registration -- the domain names that were used to send out this spam were false, and the registration behind them was false. They would have addresses where they would put numbers on streets that may have existed in Raleigh, but the actual address number didn't. So, they would put a nonexistent address

number.

Our investigators, after a while, were starting to figure out, wow, there is no building. This is a vacant lot, there are no buildings sitting here. They were obviously trying to avoid detection. But what did get them was the money, and people had to send them money, and they were using a Mailboxes, Etc., and they were -- they had actually put real information, when they registered for that mailbox, because they wanted to go pick up their money.

And I think as John mentioned yesterday, we actually had the owner of the Mailboxes, Etc. come in and testify as to who owned these mailboxes. So, we were able to trace that money back through that way.

But we -- this case is now on appeal. He was convicted and a jury ultimately sentenced him to nine years in prison, and the judge upheld that recommendation. So, that's a nine-year active sentence this guy is getting, and now it's up on appeal. It's up to the Virginia Supreme Court, and some of the issues we're facing right now that are very relevant -- two of the biggest, I won't talk about them all, because I'd bore you to death.

One is jurisdiction, and, you know, can we bring this guy into Virginia, since he was in North Carolina,

and prosecute him under Virginia criminal statutes? Well, again, fortunately, all of AOL's servers are located in Virginia, and so we proved at trial that he knew or should have known that AOL was headquartered in Virginia and their servers were located in Virginia, because all the spam he directed was to aol.com customers. They were to AOL customers. So, the spam necessarily had to route through Virginia.

But you could see how this could be a problem for other states who don't have a major Internet service provider where all their -- where all the spam necessarily has to travel through Virginia, and that's, of course, why the CAN-SPAM Act is so important as far as a criminal enforcement mechanism, because you don't necessarily have these jurisdictional issues. You can always find a victim, an end user of the spam, who actually clicked on the spam, but you're not going to get the bulk requirements you need for the statute, the tens of thousands a day.

And, in fact, you can prosecute it. In Virginia, you could prosecute based on one user receiving the email, but it would just be a misdemeanor, and as I told you, this took up our resources for six to

CAN-SPAM, you are going to hear more about that from Mona and all these guys and Keith on the federal side of it. It is very important as far as jurisdiction goes, but this is an important issue we're litigating in the appellate courts right now.

The other issue is First Amendment and free speech, which he has raised. He claims in the appeal that he has a right to speak anonymously, that -- that -- and what he does, he compares this -- in his appellate briefs, he compares this to The Federalist papers. If you remember from history class, The Federalist papers were published by Madison, Hamilton, and John Jay, but they were published with a pseudonym. They weren't published under their names. And I think it was, like, Pugilus or something was the name they put on as the author.

So, he's claiming, well, you know -- and he's right. There is a general right to speak anonymously, but there's one key distinction here, and you can distinguish it from The Federalist papers. These guys are trespassing on private computer networks to get their -- you know, send their junk commercial email out. That's a big difference. So, this is more of an actual computer trespass case than it is a First Amendment

this guy was violating AOL's policies by sending out these thousands of emails over their network, violating their terms of use, and it was their private network. So, that's going to be probably an important precedent-setting decision out of this case, hopefully on our side. We won in the Court of Appeals. It's at the Virginia Supreme Court, and there's an opinion issued.

But the last thing, which isn't necessarily a legal issue, is the cooperation with ISPs, and you will hear Aaron from Microsoft speak that it's very important to have good cooperation, especially -- well, federal and state for developing these cases, because we can only do but so much, and they have to -- they are the ones who initially bring the case and bring it to us.

And unfortunately, now, most of these operations have moved internationally, and you're going to hear,

have several more actions to announce by the end of the year.

And then I am going to talk briefly about the Botnet Task Force, and then lastly, very quickly, talk specifically about stock spam pump-and-dump schemes and why they are so prevalent right now and what types of specific law enforcement challenges they pose.

So, as for botnets, most of you probably already know what a Botnet is, but in short, it's derived from the words "robot network," and it is a network of what now we're seeing hundreds of thousands of computers essentially infected with Bot code that dial in, usually phones home through a command and control server, or now they're getting much fancier with how they're using -- it used to be Internet relay chat channels -- the mode of dialing into the main command and control server can change over time.

But basically you have 100,000 computers that have code on them. They phone in through an IRC channel to a command and control channel, and the Bot herder will issue command to the bots that are online at that moment and tell them to do things like send spam. Right now we're seeing them used not only to send spam, but also by adware affiliates, to install adware en masse.

And we are also seeing bots used to commit

basically cyber-extortion, cyber-rivalry, by committing distributed denial of service attacks from one online competitor to another online competitor, and essentially what happens is the bots are programmed to flood the IP address of the competitor to take the competitor offline. So, those are the three really popular ways that we're seeing bots used right now.

And the reason that botnets are such a popular cyber-crime tool right now is because they are, as Lois intimated, very readily available. There's a marketplace for them to either -- either buy or rent a preexisting Botnet, and it's also, we're seeing, relatively easy to customize your own Botnet. You can see postings for people looking for coders. It does not take much to get a Botnet up and running. It's not expensive, and the access is there.

And so it's a very popular tool for cyber-criminals, because you can commit very lucrative crimes fairly quickly on a pretty widespread scale, and it poses obvious law enforcement challenges, because typically, the Bot -- the infected Bot does not know that -- the consumer doesn't know that he or she is infected. There is no -- typically, there is no major indicia of infection with the infected Bot computer. So, they don't complain.

It's not like a brick and mortar, somebody got assaulted and they called the police or called the FBI. The bot -- the infected bots have no clue that they have been infected, and they can't really self-identify. It's not like we could issue some kind of a disclosure about some Bot signature and they could scan their computers and try to find the Bot code themselves and eradicate it. So, we don't really get complaints from consumers the way we do in other kinds of brick and mortar arenas, which makes partnering with private industry, ISPs, Microsoft, the antivirus community, the anti-spyware community, anti-spyware sort of vigilante groups, they start playing a more and more significant role in making law enforcement effective, because they are often the first people who have information about what's going on in the networks, whether there's a Bot going on, what it's being used to do, and they're also -- so, they can notify us, and they can also give us our investigative tools to help us investigate the Bot, whether from an undercover standpoint or using cooperators or whatever.

And they are often in the position to be first responders, so they're best able to, you know, working with law enforcement, stem the flow of the injury. So, partnering with industry in the Botnet cyber-arena is

extremely pivotal, and that is -- the Botnet Task Force that Microsoft is very involved in is one prime example of very effective industry partnership with law enforcement, both national and international.

And in -- over the course of the last, I'd say, year or so, DOJ, through various U.S. Attorney's Offices all over the country, has been investigating a variety of different Botnet cases, and they fall generally into those three categories. They are botnets used to spam; they are botnets used to install adware, and sometimes spyware, mostly keyloggers and things like that; and then they're using botnets to commit DDoS attacks.

And the obvious -- the obvious value of a Botnet and a proxy in the spamming context is that you could send 100,000 emails in ten minutes through 100,000 different IP addresses, making it much more difficult for the blacklisting and anti-spam filters to work, and also making it difficult for law enforcement to find out who you are and who the actual sender is. So, it's very popular.

And proxies are sort of the kissing cousin of botnets. The difference really -- whereas a Bot has actual malware that's installed on the machine, the box -- the box has code on it that is basically telling the infected machine to send spam or, you know, ping an

IP or install adware.

In the proxy context, basically what the spammers do is load -- you know, typically they would link up to a live link on the Internet that they are selling or renting tens of thousands of proxy IP addresses, every hour they get fresh proxies, and they buy them, they're fairly cheap, and their software program will literally stream in the lists of proxy IP addresses, and, again, the same with the Bot -- the same with the Botnet. The spam gets sent out -- it ricochets off 100,000 different IP addresses instead of the one true sender's IP address and makes it a lot more difficult for anti-spyware -- I mean, anti-spam filters and blacklists and other spam-blocking techniques, and also makes it difficult to identify the sender.

So, bots and proxies are very in vogue right now in the spamming community and elsewhere, and Operation Bot-Roast was announced June, I think, 13th or 14th, and we highlighted three particular cases.

One case, the Soloway case, was in the Western District of Washington. That was a spam case. The defendant was indicted and charged with CAN-SPAM violations, wire fraud, mail fraud, money laundering, I think that's about it, and they were using both proxies and bots, apparently, to ricochet tens of millions of

the Bot is a specific type of computer or is basically conveying certain types of information, then you have a different type of violation under 1030.

So, the third case was the Brewer case, and that involved a network of hospitals in the Chicago area, and they were noticing that their machines kept going offline and rebooting and going offline, and they did some internal testing, and they realized that they had a massive Botnet infestation on the hospital computers, and it was -- they spent thousands of hours and tens of thousands of dollars trying to identify what was going on and eradicate the Botnet. And so they were indicted under 1030, I believe it was a -- I think it was a single 1030 count in Chicago.

So, those are the three cases. There are some other cases coming down the pike, so stay tuned. The one interesting thing is that, you know, in terms of who is running these botnets and who are the potential targets for current and future prosecution, you know, there's the obvious Bot herder target, the person who's out there making the code for themselves or for hire, for somebody else. There's also the obvious customer. Those people are committing crimes, because they're the spammers who are either hiring the Botnet -- the Bot herder, or in some cases, they're actually basically

paying a coder to make their own Botnet.

There's the spyware/adware company who's also buying and utilizing the Botnet. Those are sort of the customers. But interestingly enough, there is also this tertiary level of Bot-brokers, and we're finding that we are going to start pegging some of those people with criminal liability, because what they're doing is there's an obvious middle man here for hooking up the customer who needs the Bot and the Bot herder who's providing the Bot.

And from a sort of international standpoint, we're also finding that although some component of the criminal enterprise is sometimes located overseas, whether it's backbone or maybe the Bot in its entirety, the command and control servers are overseas possibly, usually are from a sort of international standpoint, [illegible]

Fortunately, for law enforcement, a fair amount of the activity is happening in the United States. So, we've been fairly successful using a variety of different kinds of techniques and also partnering fairly extensively with private industry and other sort of vigilante groups -- and I mean that only in the nicest sense of the term -- we've been very successful in finding botnets. But the one case that was not publicly discussed so much yet, but there was a Botnet that had 900,000 bots in it, and so this is a -- this is a problem of pretty epidemic proportions, and that is why we are spending a lot of resources talking about and prosecuting botnets.

And in my remaining few minutes, I wanted to just segue into a particular type of spam. This isn't -- it just so happens that stock pump-and-dump spam is being used very regularly right now through botnets, proxies, and other methods that violate various federal criminal laws, and one of the reasons I wanted to talk about stock pump-and-dump spam schemes is because they really pose kind of a unique law enforcement challenge, because first of all, the -- unlike the normal spam where there's a click-through or there's a return purchase or there's a money flow, like you were talking, Gene, how you can usually follow

the money to get back to the spammer, in the stock pump-and-dump scheme, you get a ticker symbol, and the victim is usually -- you know, it's a very thinly

just the "why's" of why is it that just flooding the market with even accurate stock pumping information, why does it work? Why are consumers responding? Why are they buying? Why is it -- why is it driving up stock prices to flood the market with spam? And he sort of documents statistically how much of a reaction there is in the marketplace over time and how it drops and how consumers are losing tens of millions of dollars. I just read an SEC estimate last week saying that they anticipate -- I mean, they estimate that 100 million spam a week are coming from stock spam, and it's 15 percent of the total volume of weekly spam in the United States and that consumers lost tens of millions of dollars last year on these types of spam schemes.

So, that's my spiel, in a nutshell. Thank you for being here today. It was nice to see everybody.

MS. GREISMAN: Thank you very much, Mona.

event possible. It's a fantastic, unifying, and leading role that the Commission is playing in bringing this community of spam-fighters together today.

We've learned a lot over the past 24 hours about the current threats, what we're seeing, and at the Internet service provider level, we see a lot of these threats every day, Microsoft, AOL, Earthlink, Yahoo! The gateways for all of this traffic coming through, this is a day-to-day reality for the business of moving mail.

I've been told I have a bias for taking action, and you've probably heard the saying that actions speak louder than words, and that's what I'm here to share with you today, is some of the recent developments on legal enforcement actions in industry as well as government, as Gene and Mona shared a little bit about.

I lead Microsoft's global anti-spam enforcement programs, which encompasses a team of attorneys, investigators, people who are skilled and experts in finding people who do not want to be found, which is what finding cyber-criminals is a lot about, and since our last gathering in 2003, which I also was not present for, we've been very busy on spam enforcement and bringing these actions to identify, pursue, and track cyber-criminals and to try to help bring them to

justice.

Microsoft has supported more than 200 legal enforcement actions worldwide, including 128 lawsuits in the United States, most of those under the CAN-SPAM Act. Those lawsuits have encompassed 357 defendants, which includes 236 individuals and 121 corporate entities. We're not doing this alone. AOL, Earthlink, and Yahoo! also have been very active bringing these suits. We've worked with them in partnership on specific actions, with Pfizer in a specific program targeting Viagra spam, working with our government partners, the states attorneys generals, states like Massachusetts, New York, Florida, California, as well as the Commission and federal investigators, FBI and, as Keith will speak about in a moment, the NCFTA out of Pittsburgh.

All of these efforts have given us a tremendous perspective on what's happening in the marketplace of spam and spamming operations, and more specifically, the

more successes for enforcement, both private and government.

But also as a result of CAN-SPAM, we've seen this innovation that we've heard so much about yesterday and some of those techniques that spammers are now using to get their mail through filters, such as rotating or fast-fluxing the beneficiary URL or the target URL, spam that doesn't contain a link, like the stock spam that makes it more challenging to target. There's nothing to follow downstream, as we say in the investigation world. There is no link to click on, no domain name to go look up "who is" information. The pixilation, the adding of the dots, all of these techniques which make it -- which are intended to beat the filter, as a technologist would say, to get through the mail -- to get the mail through the filter, also makes it more challenging for investigations, because we're also using tools to try and bucket this mail, to identify trends, to identify the people, the person behind that computer hitting the "send" button. So, these same techniques also make it more challenging for enforcement.

As I mentioned, downstream targeting is less and less of a viable option, as there is no link in the mail to follow, and stock spam is a great example of that. As there's no product contained in the mail, there's no

money trail, there's no test purchase that could be made, another technique that investigators use, that also is a growing and current challenge. And because so much mail is sent through infected computers or open proxies, as they used to be called, now manufactured proxies or intentionally infected computers, spam trap accounts are less effective as a tool to identify the source of that mail, because so much of that mail, almost all of that mail, is now being sent illegally through infected computers, and so that requires innovation on the side of targeting and on the side of

in this space are absolutely essential to success.

In addition, international cooperation is absolutely essential. Cyber-crime knows no boundaries, and as the gentleman yesterday suggested, we like to see more people with raincoats over their heads coming out of the courthouse in an arrest and indictment, in an orange prison jumpsuit, in an international setting requires international cooperation, and so having that framework in place for information-sharing within a framework of the law that permits cases to be built and to be brought is absolutely essential, and so we're looking to tools like the London Action Plan, like the new U.S. Safeweb Act to help foster those relationships and permit those international cases to be brought more often and more frequently, because going forward, that will become increasingly important.

Microsoft, in closing, remains absolutely committed to continuing the fight against spam, phishing, other cyber-crimes, to protect our customer, to help make the Internet a safer place, and we look forward to working with you and the Commission to help achieve those goals.

Thank you very much.

MS. GREISMAN: Aaron, thank you.

(Applause.)

MS. GREISMAN: I think we have heard a whole lot about the NCFTA from a fairly high level. Can you drill down and tell us really what's going on in Pittsburgh?

MR. MULARSKI: Definitely. I'm glad to be here today. One of my colleagues was here yesterday, Tom Grasso, and I want to talk to you a little bit about what's really near and dear to our hearts, Tom and mine, so I'm going to tell you a little bit about what the FBI's doing to combat this problem so that you can get a better understanding of what we're doing.

As we spoke over the last couple of days, a lot has changed in the last couple of years since the last meeting. A lot has changed in the FBI since the last meeting as well. For one, we split up our own cyber-division now. We had -- although we worked cyber-cases before, in the past, what we've decided is we have our own division now. So, we added another layer of bureaucracy through it up there, but actually, believe it or not, cyber-crime is the third priority of the FBI, investigative priority, only behind counter-terrorism and counter-intelligence. So, cyber-crime is the number one criminal priority of the FBI. So, that just goes to show you how serious we're taking this.

We did a survey last year, because the FBI loves

statistics and loves to do surveys, so we did a cyber-crime survey, and we had 639 companies respond to us to tell us basically what the problem is, how much are you losing to the cyber-crime problem. So, 639 companies responded, and out of those 639, over 80 percent of them had experienced some loss from cyber-crime, and those losses, for the 639, were $130 million. As you know, that's just a small, basically tip of the pin, of companies doing business on the Internet.

The number one problem that those companies reported to us where they experienced the most loss, which was $42 million, was from viruses and malware. As we all know, the viruses and malware are -- they're the main thing for spam, to blast out the spam. So, that was a real eye-opener for us.

Our Internet Crime Complaint Center receives over 22,000 complaints a month for online cyber-crime. That's up from 18,000 complaints a month from last year. If you just look back a couple years ago, you know, you had a dial-up connection in your house, you know, you were lucky to have high-speed. Now, everybody has wireless Internet access. You have your phones. Everybody's looking at their BlackBerries. This is just going to proceed further and more. If we don't address

it together, it's just going to get worse.

So, what are we doing as the FBI? One of the things that we've done is we split up cyber-squads in all 56 of our field offices. So, we have a special squad of specially trained investigators, trained only in cyber-crimes, to attack these complex problems.

In addition to the cyber-crime squads, we also have legats overseas, and those are all representatives in the many embassies, and in those important embassies where we feel that we need the most attention, we also have cyber legats. So, those would be our agents that are trained in cyber-crime working together with foreign law enforcement, because as Aaron said, there's no boundaries in cyber-crime.

But as we're looking at crime, really, in the next seven to ten years, really, all crime that we're going to be investigating is going to have some kind of a cyber-element to it. Traditional organized crime, traditional bank fraud, is all going to have a Botnet-related or a computer-related thing. So, we have to adapt to that, and with that is -- you know, as Aaron had said, the problem is bigger than any one agency or any one company to attack, and the only way that we could do is to effectively partner together.

Well, this is a thing that's near and dear to my

heart, is we've established a non-profit organization, we're one of the founding members, and it's called the National Cyber Forensics and Training Alliance, and it's in Pittsburgh, and what -- together, what we've done is established a neutral space where law enforcement, industry, and academia can come together and actually work elbow to elbow to tackle these crimes, because as the FBI, all of the subject matter experts out there, you are in the trenches on a daily basis. To try to train agents to learn what you know would take years, and it's just impossible, but you can come and sit and work with us and show us what you're seeing, we can tackle it together.

So, what this does is it establishes a neutral space where we can collaborate. We can have a two-way exchange of information, and believe it or not, we do share information back and forth, and we could leverage the exponential resources that we each have to combat this. So, what we do is we try to establish a case, and then we refer it out to the -- to the law enforcement agency that we think will best work it, whether it be the FBI, foreign law enforcement, the Secret Service, the FTC, the SEC, it doesn't matter to us. We just want the case worked.

And so what we are doing at the NCFTA is we are

not, as the Government, coming to industry and saying, "Hey, this is a problem." We want industry to come to us and say, "This is the problem," and let's work it as an initiative. We have to be proactive. We can't be

of the broader aspect of cyber-security or critical information infrastructure protection or CIIP, and we sort of see spam as sort of a subset, and we have sort of a wide program of activities to assist developing countries. The International Telecommunication Union and an intergovernmental organization with about 191 member states, and if you think you have difficulties in developed countries, highly developed countries like the United States, you can imagine what the poor developing countries are faced with these days, particularly as they have very, very poor connectivity to the Internet. You know, many -- many U.S. universities have far better connectivity than an entire country in Africa or something like that.

For example, Africa has about 900 -- 900 million people, I can't remember exactly, but they have less

cetera, et cetera.

So, I've only got eight minutes, I'm told, so I should try and concentrate on just a couple of things that we're looking at. One is -- well, the first is in the concept of enforceable codes of conduct for Internet service providers, for ISPs, which we think could help level the playing field in dealing with spam, and the second is a zombie botnet mitigation toolkit that we're working on.

Enforceable codes of conduct first. When we started -- once a number of countries started passing legislation around the world to deal with spam, we made some surveys, and our last survey we did was until the end of 2005, and there was only about 23 percent of countries in the world who had adopted some spam legislation. So, that means that there's over 100 countries out there who have absolutely nothing.

And we noted that even when there was legislation on the books, even some developed countries and even some developed countries who were going around lecturing people about how they should pass spam legislation -- and I'm not talking about the United States, I'm talking about another developed country -- they actually didn't prosecute any spam cases. You know, the group that was doing the prosecution said,

"Well, we actually don't have resources to do this or we don't have the forensic expertise," and so on.

You know, I'll take the case of Sweden, you know, they had 75,000 complaints last year about spam and not one case prosecuted, to my knowledge, and it could be argued that the only thing worse than not having any anti-spam legislation is having spam legislation and doing nothing about it afterwards.

So, if developed countries have such a hard time marshalling the resources to get these things done, what chance does a developing country have, which has very, very poor capabilities and so on? And so we were thinking about this some, and we kind of got -- came around to this idea of using what we call enforceable codes of conduct for email service providers, and that was based on some country experiences that we had seen.

For example, Australia has a world-renowned anti-spam law, and they use these concepts of codes of conduct for ISPs, and the way this works basically, it's sort of a public-private partnership type thing. You go to the ISP community, you say, "Please come up with a code of conduct of how you are going to deal with spam and spammers, and you absolutely swear that you won't host spammers, et cetera, et cetera, and then we're going to back that up with a regulatory backstop," okay?

would look at this in a totally different way.

and this is another one of these public-private partnership things. It's a public partner -- public-private partner for watch, warning, and incident response. Basically the way it works is that the spam regulator in Australia is actually the communications and media regulator. Who is a spam authority in different countries depends very much on the historical

quite a bit today about -- and yesterday -- about the general challenges of dealing with spam. As Aaron put it, I think, finding people who don't want to be found, and -- but here, I want to focus on the sort of aspect of the "Where is Waldo" game here that when we start crossing borders and the increased challenges that that adds to -- from the point of view of enforcement.

As I think Suresh mentioned yesterday, generally a lot of the spamming techniques can be used pretty much from anywhere, and this kind of -- some people have used the epidemic analogy. It's an epidemic where you can't easily seal the borders. It's where you have the wrongdoers or the victims, the evidence, the servers, these can be anywhere. They can be in a combination of

are the same challenges that we see in doing a lot of fraud enforcement work from the point of view of needing to cooperate across borders, needing to have the right tools to work with others to bring effective, coordinated, international efforts. I think Joe St. Sauver made the provocative comment Lois referred to of the methods of international cooperation being primitive, which I have to admit put me in a kind of iron-age mood yesterday, but I think that it is at least true that we're in a tool-building phase here in terms of developing the kinds of coordination that we need to have.

Joe also suggested that this requires coordinated international effort and that the United States should take a leadership role, and I think that the United States -- and we heard the FTC -- have tried to do that, and they have focused on sort of two basic issues. One is developing our own or building our own capacity, our own tools, to pursue the international cases, and then second, to work together cooperatively so that we all, together, build the ability internationally to have the capacity and ability to cooperate.

So, to start at home, the FTC has focused a lot of effort and testified on the need over the years for

legislative changes to improve our ability to cooperate and made a legislative recommendation, complete with cover art here, for legislation on what Congress passed as the 2006 U.S. Safeweb Act, which I'd point out, part of the acronym there is undertaking spam, spyware and fraud enforcement with enforcers beyond borders, and so one of the challenges here with spam, as with other kinds of cases of various kinds of fraud, is for us to

Then, moving to the international environment, there are, of course, a number of challenges here, and Bob Shaw actually referred to some of these. You have some places where you don't have an agency or you may have an agency that doesn't really have the legal power to investigate or to take action and/or to have remedy, or you might have an agency that theoretically has the power to do it but no experience in bringing these kinds of cases, and you have, as I think Bob also mentioned, different kinds of agencies in different places working on these cases. It might be a telecom regulator in one place, a data protection authority in another place, a consumer protection authority in another place. Criminal law enforcement agencies might play one role in one country and a different role in another, and that whole environment makes it a challenge to cooperate.

In addition, just basic communication. How do we communicate, not just through language barriers, but other barriers, different legal traditions, different approaches, and how do we deal with those challenges? Some of the response at the international level there has been to try to coordinate a little bit the general direction in which we take these efforts, and at the OECD -- this is the Organization for Economic Cooperation and Dani0.000ECD -- this is t0 0dit

developed economies, there has been work done to put together a toolkit on spam, and part of that has been a toolkit -- has been a recommendation on spam enforcement.

And as with cross-border fraud enforcement, there's certain basic sort of tools that folks need, such as basically have some domestic capacity to bring cases there. If you can't bring your own case, it's difficult to cooperate with others in bringing an international coordinated case.

We have also, at the FTC, done a number of memoranda of understanding, coordinating with agencies in other places, partly to develop more of a conversation about how we can proceed and take next steps in the area of cooperation, and there have been some cases where we have been able to share information and cooperate, but also, part of this is also getting to know the regulators, to know how we can talk to each other and how we can coordinate.

This is not really part of the FTC's ambit, but I probably should mention the Council of Europe Convention on Cyber-Crime, which is aiming at the -- on the criminal side to provide more tools for cooperation, and that's also sort of a development in the network of conversations that my criminal enforcement colleagues

could also probably comment on more, better than I.

The other thing I wanted to mention is the London Action Plan, which I think Bob and others had referred to briefly, and the effort there was really to start the conversation between these agencies of different sorts so that we could really figure out who should be involved, bring in the appropriate industry players, and have that conversation, and this has been a range of countries involved there, from -- in some of the developed economies and also others with agencies or folks who are interested, from Chile to China, we have had a range of participants there, and there have been some initiatives there.

In 2005, for example, there was an initiative on educating ISPs about botnets or, as we said then, spam

get set up, and we are hoping that we can continue that kind of conversation there. This is a building process that takes some patience but is really what's necessary to develop effective international cooperation in this area.

Thanks.

MS. GREISMAN: Thank you, Hugh. We do have time for questions and answers. I'm going to exercise prerogative as moderator and start out.

You know, Hugh, you asked, where is Waldo, and I'd like to go back to, who is Waldo, and Gene, you showed us a mug shot, and Mona, you spoke of Bot herders, Bot brokers, spammers who hire them, and I think you and Keith both referred to them as fairly sophisticated, intelligent people.

Can you give us a better profile of who these people5a C(14 eu Yotf who these)TjET1.00000 0.00000 0.00000 1.

as Mona pointed out, are sophisticated and have pretty fairly sophisticated business models set up, and the reason for that is -- I mean, these guys, they're pulling in -- the most egregious are pulling in millions of dollars, and that -- you know, they have virtually really little overhead, relatively speaking. So, it allows them to set up these movr9eTe1.0and the

to someone in the States and planning their scheme on computers they are going to infect, stocks that they are going to manipulate, and it's really a new and emerging threat that we really need to understand and grasp. So, I really think we need to look at it from an organized crime standpoint and change our view on that as well.

MR. KORNBLUM: The senders of illegal email are greedy, and they're needy. They're greedy, as Gene points out, they're in it for the money. They're in it to make money through the transmission of the mail and the return on their investment, but they're also needy. They also need a lot of things to make the whole ecosystem work. So, they need a web host for that domain; they need that series of open proxies or manufactured proxies to get the mail through; they need, if they're selling a product, they need to fulfill that product and have someone shipping things through; they need to move their money. So, they're -- those are their weak points for investigations, and where we're focusing on is focusing on those needs, because they tend to be the weak links in their systems and in their operations.

MS. GREISMAN: And that actually raises the next question, you know, without divulging any state secrets, what are the investigative tools that you can speak

about, and what have you found to be very effective or perhaps less effective?

Keith, why don't we start with you.

MR. MULARSKI: Okay, throw me to the fire.

Well, I think that there's a number of different things, and it all starts by you have to look at this as an intelligence case. You have to look at the organization and gather intelligence as much as you can about the person. So, by that, leveraging the subject matter experts, if we're talking about a spam case, the different ISPs that are receiving mail in their

MR. KORNBLUM: I'd just say that even with the electronic resources in hand, you need those gumshoe, traditional, investigative resources. You need that in-house capability to put the case together to take it to a judge, because at the end of the day, you need to bring a case into a courtroom and say it was this person at this time who pressed this "send" button to move that mail or to launch that virus or to send that Bot out. So, having that aspect and that capability is absolutely essential as well.

MR. MULARSKI: And one thing, just to add on that as well, is as we've talked about foreign -- foreign countries not really being caught up with the laws that we have here. So, when we go and we package a case, maybe we don't package it as a spam case. Maybe we package it as a fraud case or an organized crime

Mona, you've mentioned installing adware en masse. Are there sort of things that marketers should be looking out for in terms of, you know, sort of typical organizations or typical elements that perhaps can tip you off, "Hey, look, this may not be so great," or can you talk to that?

MS. SPIVACK: I would say -- yeah, I mean, I -- let me just give a little bit of background for those of you who may not know how this sort of adware/Botnet thing works, but basically what we're seeing is that the Botnet is used -- you could have, let's say, 50,000 infected bots in a network, and the adware affiliate is actually the customer of the Botnet. So, the adware affiliate is going to be paid by an adware company per install of a particular piece of adware code, and the adware code could be somewhat -- relatively garden variety, benign code that showed some pop-ups, or it could be, you know, a homepage hijacker, or it could be -- it could install spyware like a keystroke logger, and they could get paid in a variety of different ways. They could get paid per install. They could also get paid per click. They could get paid per impression after you've got the code on the infected Bot. Every time it serves a popup, the adware affiliate is getting paid, and every time the customer actually clicks on the

popup, they get paid even more. So, it's a way for a sort of crooked adware affiliate to make cheap money, and arguably, it's defrauding the actual adware company, because they're not really getting legitimate eyeballs and legitimate -- it's sort of click fraud on the adware company in some ways.

And I would say, you know, just from a practical standpoint, if I were an adware company and I was trying to figure out are my affiliates using botnets to install adware, I would look at the numbers. It's hard to socially engineer 10 million installs. It's hard to get a consumer to read a EULA and click "okay" and say, "I want this code," to the tune of $10 million. I would say that, you know, if you have some one-off affiliate who is just churning out a lot of installs, I think that's a pretty good indicator that there might be something amiss, and I would want to go have some serious conversations with my affiliate and consider taking steps and also notifying law enforcement.

But I would -- I think other than sort of the -- the sheer numbers usually are the biggest early warning sign.

MS. GREISMAN: There was another question in the

I wondered from Mona and Keith what RICO does for you, if anything, in investigating and prosecuting these.

MS. SPIVACK: Well, the problem with RICO is that you have to have a certain type of predicate act to bring a RICO charge, and CAN-SPAM violations at this point, my understanding is, do not fall into -- they are not a cognizable predicate act for RICO.

Now, you can often bring wire fraud charges, which have pretty enhanced penalties. You can dovetail -- once you have wire fraud, wire fraud is what they called a specified unlawful activity that will trigger money laundering, so then you can bring in money laundering, and CAN-SPAM also has its own asset forfeiture provisions, so you can really hit them where it hurts by seizing all of their assets.

The other thing that I would say is the sentencing guidelines -- although after Booker, they're not mandatory, but judges are still looking at them -- the sentencing guidelines have some enhancements that are very helpful in CAN-SPAM prosecutions. For -- you know, for example, if you have a sophisticated means that you're using, if you have a certain number of victims, if you harvest email addresses, you get a bump in your sentence. If you are -- in the Soloway case,

actually, I think they even brought an ID theft charge under --

MR. KORNBLUM: Aggravated --

MS. SPIVACK: -- aggravated ID theft, which is 18 USC 1028-A, which gives you a mandatory two-year bump in your sentence, because what was happening was the sender was -- they were falsifying the "from" addresses, and they were putting an actual person's name in the falsified email address, and -- and they charged them with aggravated ID theft, and that has another sentencing hike.

But RICO, as it stands, is not available to us. That's my understanding.

MS. GREISMAN: Thank you. Let me direct a question to Robert and Hugh. Let's move out of the stone age. Let's work our way through the Renaissance and plow right ahead into the age of enlightenment.

Where are we going to be? What is the world going to look like two years from now, three years from now?

Robert, why don't we start with you.

MR. SHAW: Oh, thanks. Stone age --

MS. SPIVACK: I told her not to ask me that question before this.

MR. SHAW: Oh, I don't know. It's terrible.

Maybe I'm getting too old. I'm a little bit cynical, because I see, in the international cooperation sphere, there is so much work to be done, and also, we still see silos of communities who really don't talk to each other, you know, Interpol has its own high-tech contact list, this group has its high-tech thing, and the mixing of spam and the broader cyber-security issues means there's all sorts of initiatives.

Hugh mentioned the Council of Europe, you know, trying to get people to sign onto the convention, and there's some countries who politically don't want to sign onto it because it has the word "Europe" in it, and so one of the things we're actually doing at the ITU is coming up with sort of model law that looks just like the Convention, but it's not called the Convention, and so to me the international cooperation mechanisms are such a massive challenge that I just -- and there's so few people actually working in the space and dedicated to those problems, I'm somewhat pessimistic.

You know, someone brought it up yesterday, I think, you know, the U.S. probably has about less than one-third of the world's international Internet connectivity, and that's because of demographics, that's just going to grow and grow and grow and grow. You know, in China, China will surpass the U.S. in total

broadband connections this year, next year, and that's where the real growth is, is in countries like China and India, and how do we cooperate with them in realtime?

And what surprises me so much, that there's a large black balling service present in this room right now, and we got a call from them last week, "Who's the person to contact in Russia for cyber-crime?" So, even the people who are working in the field, who are experts and working in this space the whole time, they still have a really hard problem finding their counterparts in other countries and getting something done in realtime, and that's a real gap, and how we solve that gap and cross these various silo communities is something that's going to be a challenge over the next five years.

MS. GREISMAN: Thank you.

MR. KORNBLUM: They should talk to Keith. They should talk to Keith for that Russian contact.

MS. GREISMAN: Hugh?

MR. STEVENSON: Well, my mother told me that patience was a virtue, and I think quite a bit of patience is required in the -- in terms of the pace of the international developments, that these things move more slowly than we would like for a lot of reasons. It's just a challenge to coordinate legislative development and political attention and the development

of experience in handling these kinds of matters.

Things, though, I think have moved forward, and566enters.

most difficult to be pursued, and it may be that there are -- as Mona mentioned, if there's certain opportunities in stock-related matters, that may be sort of where the things gravitate.

On the demand side, we -- the kinds of issues, particularly at the Federal Trade Commission, we deal with, until we run out of people who, you know, who don't want to get slim fast and rich quick and borrow money easily, that there will be sort of areas or targets for people to develop, and so I think it's hard to predict where that will be, and I think we've seen that in other analogous areas, such as, for example, telemarketing fraud or web-based fraud.

MS. GREISMAN: Let me address one of the questions submitted and actually start with Gene on this.

A person asks, it sounds as if there's an extensive infrastructure selling needed services to spammers. Is there a way law enforcement can deal with that infrastructure?

MR. FISHEL: Well, yeah. I mean, I think that's -- you know, that's a bear, and when there's a lot of money involved, there's going to be an extensive infrastructure, but I think as -- I think Aaron was saying, you know, a lot of this just comes down to -- to

think about a couple of dozen stocks, that they pulled the listings from.

And the second thing is, of course, that we keep coming back to the money trail and money laundering here. There are, of course, far fewer avenues that spammers and Botnet people are regularly using to transfer money around, and they have now taken to hijacking existing resources. I think we have somebody from the U.S. Postal Service around who will probably be talking about mail fraud and money transfer. There's Western Union and there's some of these shady online money transfer services, like E-Gold.

MS. SPIVACK: E-Gold.

MR. RAMASUBRAMANIAN: The mainstream credit card vendors do have to get in with this, and you've got the (inaudible) and other international financial fraud people, but we certainly need to start talking a little more to them than that's been going on.

MR. FISHEL: Just a quick comment on the E-Gold and those kinds of services, those are -- those raise problems. We do a lot of child pornography, child exploitation cases in our section, and E-Gold's used to purchase pornography off web sites, and it's just -- it's just been a problem, because they disavow any knowledge of what goes on --

MS. SPIVACK: Although our section indicted E-Gold last month, so they are currently under indictment, so --

(Applause.)

MR. FISHEL: Good.

MS. GREISMAN: Aaron, let me shift a question back to you. You spoke of 128 cases that Microsoft has brought and the general benefits of private enforcement, the limited private enforcement under CAN-SPAM affords and, you know, separating the really bad guys from the maybe not so bad guys. How do you assess the impact of those cases?

MR. KORNBLUM: Well, it is difficult, as I think someone said yesterday, to put a lot of stock in statistics, whether it's number of cases or number of

know, you need someone to have a facilitation role, and that takes a recognition at a high political level. So, that's one of the things that we're working on a lot, is trying to assist in the development of national strategies there, and then -- you know, of which cyber-crime is one component and watch warning is another component and spam is another component.

MS. GREISMAN: Keith?

MR. MULARSKI: I think it's that we realize that we could share information between one -- each agency and that we can work it together to get success, and we're recognizing that if we do that, that we can maybe make a dent in this problem.

MR. KORNBLUM: Enforcement is part of the solution. We're going to hear I know more this morning and this afternoon about the technology and some of the other solutions to help stop the spam from getting through, but on the enforcement aspect of the comprehensive approach, working together, we can do so much more, and I think we've seen that the most impactful prosecutions have been built on partnerships like the Jaynes case in Virginia, the Soloway case in Seattle. It's where you're sharing that information and building on the expertise of industry, the investigative power of government, that that's where the maximum

impact can be delivered.

MS. SPIVACK: Well, I think bringing more and more criminal law enforcement actions against spammers, who are clearly committing crimes based on the techniques that they're using, and getting stiff jail sentences and using the asset forfeiture provisions. I think the one-two punch of a healthy dose of jail time plus lose your money is working, and I think in the coming months and years, you'll see it working more, and I hope that that provides a deterrent effect to other would-be criminal spammers out there.

MR. FISHEL: Yeah, I think from our point of view, two things: As Bob was saying, I think more legislators are realizing the growing problem, and so at least in Virginia, we're developing new tools within the laws to go out and prosecute these guys on -- for several different offenses, not just spam, but fraud, and I think there's been more recognition and even enhanced penalties, at least in Virginia and hopefully federally, for these crimes.

And also, probably the key thing is, as these guys mentioned, the cooperation between -- you know, from a state perspective, with federal agencies, and the Internet service providers, because we couldn't do it without them.

MS. GREISMAN: Thank you. I did not get to everyone's written questions, so I invite you to approach each and every panelist afterwards. We will be taking a 15-minute break, and please join in a round of applause for the panel.

(Applause.)

(A brief recess was taken.)

KEEPING IT OUT OF THE INBOX

MS. CHRISS: Okay, everyone, let's settle in. Let's settle in and get started here. Mixing and mingling, but now let's talk about keeping it out of the inbox. Ultimately here we do want to protect consumers. We want to protect their inboxes. So, we're talking about spambots, malware, viruses. The issue now is how to make sure these terrible things never even reach the consumer's inbox.

I'd like to introduce this very distinguished panel of experts. I have Craig Spiezle. Craig is the director of online safety, strategies, and technologies with Microsoft, and he wears many hats. He's also the executive -- to say the least. He's also the executive director of AOTA, which is the Authentication and Online Trust Alliance.

Jim Fenton is a distinguished engineer in Cisco's technology center, and he's one of the co-authors of the specification for Domain Keys Identified Mail, which I understand we have some very exciting things to discuss with that, Jim.

Next to Jim we have Des Cahill. He's the chief executive officer of Habeas, Inc., which is an email reputation services provider.

Next to Des we have Ken Hirschman. Ken, thank

participate here today and the kind introductions, but humt sounds like you should bey ay anouncer fFora baseballt

Laughter.)t

some technology investments, and we'll talk about Sender ID, reputation, and postmark programs, which I think others will touch on, and phishing technologies as well, and industry best practices. I think it was summed up real well on the last panel about the key to this is the collaboration. The problems are bigger than any one company, and the need for us to really collaborate, share best practices. It takes a village, and clearly this is an area we need to do that. We're seeing the results in enforcement. We're seeing the areas in industry collaboration and such here.

So, my slides are going to very quickly go through here. The challenge that we have is what I call the three Vs, it's the volumes of the threats, the attack vectors, and the velocity of change, and so as we've heard the cunning nature of the online criminals continually change very quickly, and our challenge is really how to protect that user and protect their PC where their data is at.

So, the outer perimeter or the first wall of defense is really the ecosystem, and a tremendous amount has been done by ISPs and hosters and technology providers, but I would submit a lot more needs to be done, and we'll touch on that, and the email defenses. So, someone has been very kind on advancing here for me.

The email defenses are a key area that we need to work on, and that's the area I think I'll share on email authentication and the success and also browser protection. We have to look at the continuum of the threat. Just because the email may get through, we also looked at what is the link that they're clicking on in and we need to have greater accountability of the links that are embedded in the email. So, it's not just the email, but it's a web site. Does the web site have spyware on it? What are the other threats that we're looking at?

So, I get asked quite often, why are we eighty-one T1.00000 concerned about email authentication? And so this is

this is -- we are all suspect -- we are all susceptible to this. It's a worldwide issue. So, this is one of the reasons why email authentication is so critical, is because we can detect this spoofed mail.

We have recently been seeing an increase, just

have, and help overcompensate really for scoring that content filter may have flagged in the past. So, that's the good news for legitimate brands.

And I'd also submit that this same approach really, whether it's Sender ID or DKIM, when you apply reputation data to the result, is really where you are going to get the results. You need to have reputation data.

So, the good news is we're now using this. We're detecting 95 percent of the phishing exploits as a result of this. So, we're finding great success, and we're blocking over 20 million exploits on a daily basis.

To give you an idea of adoption, where are we today, I'm happy to announce that we're now at 45 percent of legitimate email is Sender ID-compliant, which is fantastic, and when you add to that mail that's either DK or DKIM, combined, we're talking about over 50 percent worldwide of legitimate email. So, that's great success.

We're talking -- actually, this slide is a little outdated. It's now closer to 12 million domains worldwide are Sender ID-compliant, and we're having great success in the financial institution and marketers. So, again, authentication with Sender ID is

providing tremendous value, and I also encourage people to consider DKIM as a complimentary solution. They work very well together, and they help compensate for each other's strengths and weaknesses. So, key areas to think about and key results of really protecting the user, and that's what it's all about.

I also want to talk about phishing filter technology. Very briefly, again, just blocking the email is not good enough, and so with Vista today and IE7, we actually are blocking over 2 million phishing site attempts per week, and so that's providing, again, another level of protection. I'm not going to get into the details here, but, again, and we're only able to accomplish this because of data sharing within the industry, and this is a tremendous asset. So, many companies such as RSA, who spoke yesterday, and MarkMonitor and Internet Identity, other companies that are providing us realtime data, is really helping us to provide an increased level of protection from these threats.

The other area I wanted to talk -- I wanted to touch base on some other best practices very quickly here. Yesterday, you heard about, again, what we can do to provide the user more control. I think someone spoke about more buttons. Trevor Hughes, I think,

specifically. Unsubscribe is one of these key areas today that we need to look at providing a vehicle for users to legitimately unsubscribe from mail they don't want to have, and so that's a good best practice.

Port 25 management. ISPs need to do more, and clearly a lot of areas there of managing their outbound mail abuses or throttling that we've had challenges with in the past, you talk about some of the bots, and it's really monitoring your infrastructure, monitoring your connections, and what we can do in those areas, provide more control and such.

obviously are going to have to make more investments ourselves.

Email authentication is really key. I think marketers have done a great first step, but more needs to be done. They need to go beyond worrying about marketing email campaigns, but also protecting the domains and brands of the companies and the other email -- the other email streams.

I mentioned before ISPs. Again, many ISPs have done some great work. AOL has been a great partner, but others need to move from the sidelines and really make some investments and control the outbound mail management.

So, again, that's my key points that I wanted to touch on, and we'll have a chance I think to discuss more in the Q&A. So, thank you.

for authenticating messages that has just been approved by IETF, and then I am going to broaden out a little bit and talk a little more generally about email authentication and amplify on some of the things that Craig has just said.

So, as I mentioned, DKIM was just approved by IETF this past spring as a standards-tracked protocol, which means that it's gone really through the full vetting process that IETF goes through when approving a standard, and what DKIM does is it provides a signature-based mechanism for authenticating an email message. We put an additional header field in the top of the message. Somebody who doesn't implement DKIM will probably not even notice that it's there, and that was a very important characteristic, that we wanted to make this play well for people who hadn't implemented DKIM as well as for those who had.

DKIM, the signatures that are used understand DKIM support authentication even when the message is forwarded through a transparent forwarded, like if you use an alumni address from your college or something like that, and it's really complementary to path-based techniques, like Sender ID, and we also advocate the use of multiple methods of authentication.

There are quite a variety of vendor email

products that are already available and many more that will soon be available that support DKIM, and this ranges all the way from products that are intended for small and medium businesses as well as those that would be used by large enterprises and service providers. Also, DKIM can be implemented perhaps on behalf of a small business by their service provider if the business wants to delegate a key, delegate the ability to sign to an email service provider or something like that, and that could be used both for their own messages as well as for outbound email marketing campaigns and things of that sort.

Google Mail is signing with DKIM, and we expect

to transition that over to DKIM support in our infrastructure as time goes by, in the next few months. We have thus far gotten valid signatures from over 20,000 domains now. That's a very small number in comparison to the numbers that Craig was talking for Sender ID, but we're, of course, much earlier in our deployment.

We've gotten a lot of good experience from that. One key thing that people worry about when they think about a signature-based technique is what's the computational overhead involved in computing and verifying these signatures? And we've found it to be very low.

So, what does email authentication really do for you? And here's where I'm going to broaden out a little bit. The easiest way to describe a benefit is that you can create whitelists and essentially deal with the false-positive problem from the known domains that you have in your whitelist that are -- that are signing or otherwise authenticating.

The other thing that it does is it allows you -- it gives you a reliable domain name, a domain name identity on the message that's reliable enough that you can have domain-based reputation systems and accreditation or certification systems. Now, that

hasn't been possible up to this point because you really didn't know who the message was from, so you really didn't know reliably enough about it in order to accumulate a reputation based on the domain name. The only thing that you really had was an IP address, and there are reputation services, a lot of them based on IP address, but IP addresses do get re-used, do get changed from time to time. If you go to an ISP and get an IP address that happens to have been associated with abuse in the past, it's a difficult problem to get that corrected.

The other thing is that it's kind of a deterrent for especially the well-known and phished domains, for the use of those domain names by cyber-criminals, and that's kind of a segue into the next topic, which is what do you do about unauthenticated messages? In order for it -- in order for email authentication to be helpful in some of these cases involving phishing or involving trying to detect whether or not the message may be abusive when you don't have a signature or it's unauthenticated, you need some indication about -- from the domain about whether the message that you've gotten should have arrived with a signature, for example, and there's an emerging specification called Sender Signing Practices that's currently being worked on by IETF

that's really intended to provide some additional information separate from the message to a verifier that allows them to determine whether or not the message that they got should have had a signature on it or would have been likely to have a signature on it.

Now, this is particularly useful for domains like those of banks, financial institutions, that have been subject to phishing in the past. Domains that sign all of their messages can publish something to that effect and make those -- make messages that come without a signature appear more suspicious.

Now, I want to be quick to point out, this is not a cure for phishing. This is an additional tool. This is something that will perhaps cause the phishers to use o00 0.ofook-aike tinancws00 13ntcion'hat have

probably going to make the message ofoo a little bit less legitimate, make people think twic about it, and so while it's not a cure, anything that reduc 13nte

beneficial.

Now, one question that get13asked a lot and one point of confusion about authentication is, well, is an authenticated message necessarily good? And the answer

feeling i13ntciouse of a different tinancws00 is

is definitely not. Cyber-criminals will authenticate their messages. They will do whatever it takes in order to make their messages look more legitimate. If authentication does that, then they'll authenticate. We have strong circumstantial evidence based on our deployment, just looking at the -- some of the domain names that we've gotten signed messages from, that cyber-criminals probably are doing that. Now, I don't have access to the messages for privacy reasons, so that's why I have to say that it's circumstantial evidence that we have.

But authentication limits the addresses that cyber-criminals can reasonably use in the messages that they send. They will still register throw-away domains, and we have to address some of the accountability issues associated with registration of domain names, and just remember, throughout this whole thing, that authenticated messages aren't necessarily desirable, but there's definitely a role for accreditation and reputation services, either locally maintained, like whitelists, or shared commercial services that will provide more information about authenticatrm7domains,

make it through. There's supposed to be a picture of a peephole.

Yes. So, a peephole provides information to the person on the inside that says -- that they can look through it and say, "Oh, it's a friend, I'll open the door," or maybe it's somebody they don't recognize, but they have a good ID card from the utility company, and they'll say, "Okay, that's fine, I'll open the door." It's somebody you don't know, so you might shout through the door and say, "Who are you and what document?" Or maybe it's somebody that is showing up that really doesn't want to be seen, wants to hide next to the door, doesn't want you to see who they are, and you should be very suspicious about those kinds of people. That's really the kind of value that we're trying to provide for email messages here.

Thank you.

MS. CHRISS: Thank you, Jim.

(Applause.)

MS. CHRISS: Des, that's a good segue for you. We just finished hearing about the importance of reputation services, so tell us what you know about it.

MR. CAHILL: Thanks for the setup, Jim and Craig, and if I can exit this.

MS. CHRISS: Just keep going forward with the --

observed and objective sender behavior. So, it's not a subjective judgment about, well, I really don't like emails from this guy, but Craig really likes the email from this guy. No, it's more objective data around how many complaints are generated when this person sends email.

End user feedback or consumer feedback is a really key component of reputation, and what do I mean by that? I mean if you use Windows Live Hotmail, you use Yahoo! you use AOL, there's that button that says, "This is spam," and that is a really powerful mechanism that has emerged over the last few years, and that button allows consumers to vote about what they think about that email. It doesn't matter if they subscribed. It doesn't matter if they didn't subscribe to the email. Is the email relevant to them at that point in time? If enough -- if a high enough percentage of consumers are complaining about the email that you or your company send, that's sending a message to you that you need to re-evaluate the practices in your email program. So, consumers are key.

Generally, when we talk about a paradigm for reputation, we think in terms of a granular score. So, the analogy I would use is that we all have a credit score for our personal credit history, whether it's

TransUnion, Experian or Equifax, we have a score of zero to 800 based on our behavior as a consumer in repaying debt, taking on debt. In the same way we think about the evolution of reputation as eventually giving senders a granular score based on a number of objective data points about them. You could think of, you know, great senders as having a 100, spammers having a zero, and then there's lots of people in between there.

Reputation covers not just good mailers, not just bad mailers or spammers, but it covers the whole spectrum of emailers, everyone from good to bad to in between. In terms of what entity is this score or reputation going to be assigned to, today, it's being assigned to IPs, and Jim talked about the issues with IPs. They can be re-used by -- sent from one company to another company, and the new company inherits the bad reputation with the old IP.

We have many sender customers that want to start sending email out of a new IP address, and they're a reputable mailer, but the problem is is that Hotmail or Yahoo! doesn't know that IP address, and they may not deliver the email from that address. So, there are issues with assigning reputation to IP. It works today, but I believe that we are moving toward more of a domain basis for reputation, and ultimately, whether it is an

IP or domain, the business entity needs to be held accountable by the reputation score.

It is a -- reputation is an important component in minimizing the impact of spam in the inbox. If you can tell who's good, you can make sure that email is delivered and filtered harder on the rest of the email. If you can tell who's bad right away, you can drop that email. What's left over is a smaller amount of email, the unknown or gray email that you need to filter.

Authentication and reputation work together. Both Craig and Jim hit upon this, but this is a really important point, and I want to emphasize this. Whether you're using a Sender ID framework or DKIM or, ideally, you're using both or planning to use both together, because they are complementary technologies, it improves the identification of legitimate email as well as the identification of spoofed or phish email.

The -- no presentation on authentication or reputation would be complete without using the de facto 2007 industry standard analogy, which is that of a driver's license. Authentication is like having a driver's license. It's like having plates on your car. We know whose car that is. We can track that. But unless you have a driving record associated with that license or associated with that car, you don't know

whether that's a safe driver or that's an unsafe driver. So, authentication is necessary, but authentication alone is insufficient. Authentication and reputation work together.

I'd like to suggest a couple of models and how they can work together. If an ISP is receiving email and that sender has a known bad reputation, well, it's easy. We know what to do with that email, and that's to drop that email or block that email or throttle that email and not let us much of that email come into the system.

If there's a known good reputation and that sender is using authentication, so we can assign that reputation confidently to that sender, then we know that we can deliver that email. So, perhaps that email goes right into the inbox without getting filtered. Perhaps it's only filtered a little bit. Perhaps you're giving more privileges to that sender, and they're sending out of a new IP address, but you trust that sender, so you are willing to let them send you email out of that new IP address.

If there is an unknown reputation or there is no authentication, then e priviltng to lewanto dolteredhat

email. It could be a spammer. There is no way to know.

Let's talk for a moment about the evolution of reputation, the origins of reputation. I would say that it began in about 1999, and the emphasis was on negative reputation, blocklists or blacklists. The first one I believe was MAPS, which became known as Kelkea, which was bought by Trend, Spamhaus as well, and the notion there was that Internet volunteers, Internet do-gooders were going to compile lists of known bad guys. In the case of MAPS, they were asking companies to give them some money. So, the business model there was that a receiver of email was paying money to know about a list of bad guys, and that got increasingly sophisticated as companies like IronPort introduced Sender-Base, Symantec introduced Information Services, Trusted Source came out from CipherTrust, Secure Computing, and so that area has evolved a lot, and in the anti-spam world, there is a heavy use of reputation systems, as well as on the ISP side.

In 2002, we saw the flip side of blacklists, and we saw whitelists emerging, and the notion here was, well, can Bonded Sender or can Habeas or other companies who were in this business, can we come up with a list of policy statements that if a sender is meeting these policy statements, they've got a low complaint rate,

they're compliant with CAN-SPAM, they generally have good business practices, those -- we are going to put those guys on a list, and we're going to charge them money to get on that list, because we're going to monitor and make sure they're compliant with those practices, and then we're going to hope that ISPs and anti-spam providers adopt those services. So, the model there is that a sender was paying for monitoring of improving their business practices and therefore getting improved delivery, and that model continues today.

Where we are today, though, I think we've evolved from just looking at things as either bad, on a blocklist basis, or looking at things as good on a whitelist basis, and we've emerged to reputation. We're looking not just -- we're looking at the whole spectrum of senders, legitimate senders that are authenticated with good reputation, bad guys that are known bad, and most senders are in between that spectrum. There are a lot of legitimate companies out there that have problems in their email infrastructure or haven't adopted authentication or haven't adopted best practices.

We're covering a lot more senders. I know at Habeas, we're covering a lot more senders, tens of millions, in a reputation database as opposed to in our whitelist approximates, we're covering thousands of

reputation information across a view of the Internet.

What is the impact of reputation on the email ecosystem? Well, it's about bringing transparency and accountability to email. If you have authentication, you've got accountability. If I know that Company XYZ is sending out email, I know all their IP addresses and domains, and I'm watching their practices, I can assign a score to them. They are held accountable. Their email delivery rates, which are important to them, are in their control. It's a result of their actions.

So, what's the impact of reputation on the email ecosystem? For ISPs, additional data sources on sender trustworthiness. For commercial senders, again, it's an incentive for them to improve their emailing practices. If they're being rated and their delivery rates are going to be lower because there's, again, transparency and accountability, we're going to see a lot more senders paying attention to their email practices.

For email service providers, understanding reputation data about prospective customers or current customers is a way of protecting their infrastructure. They want to know if they've got a customer that's engaging in poor email practices, because it's damaging the reputation of their IP addresses. Most importantly, for consumers, consumers are now empowered to make

choices about email.

Due to CAN-SPAM, they can be sure that for legitimate email they're going to be able to opt out of that email. They have the power of the "This is spam" button to vote on email they don't like, and industry best practices say that consumers should opt in and give permission. There are many senders that obey CAN-SPAM and the opt-out paradigm, but those senders have, I would say, generally poor reputations and get poor ratings from consumers in their email practices.

Let me close by giving a little context, share some data around reputation. So, we analyze email traffic. We have been doing it for about the last 18 to 24 months. We've got about 5 million email networks around the globe that report email traffic data to us that we analyze every day. We're seeing about 800 million queries a day at this point, and we test all of those IP pairs, all of those senders, we test them in areas of identity, reputation, infrastructure, and practices, all tests that we feel are important in terms of determining the reputation of a sender of email.

What we saw in June of 2007, we saw 750 million distinct senders of email, 750 million distinct IP addresses sending email. 450 million of those IP addresses were dynamic. So, those were probably bots.

Throw those away and take 390 million static IPs who are left that are sending out volumes of email. Of that, of the 705 million, 99.8 percent of those senders, according to our tests, were classified as having a reputation of a spammer. So, they were either dynamic or they were a static IP that failed multiple tests, if not all the tests. So, the job of the ISPs in finding legitimate email is extremely difficult.

Of the non-spammer senders, of the 0.2 percent that were left over or 1.5 million senders, we classified only 40,000 of those IPs as good senders that passed all tests and that had a really solid reputation. That doesn't mean that among the 1.46 million that were left over that there weren't legitimate companies. It just means that of those 1.46 million, they had not -- they had either not adopted authentication or they had adopted authentication, yet their emailing practices in infrastructure or CAN-SPAM compliance were poor.

Of the 1.5 million non-spammers, we saw 27 percent using Sender ID framework on SPF, but 13 percent or roughly half of that 27 percent had their records misconfigured, and of the 1.5 million, over 40 percent had reverse DNS issues.

So, conclusions, there are a lot of spammers out there, and it's really hard for AOL or Hotmail or Yahoo!

think adding a symbol confirming authenticity is important. This was in the context of users who say, hey, my ISP does a great job of trying to filter out, you know, bad spam, puts things, you know, in my spam folder, but what I'd really like to see is some indicator that, in fact, an email is good, which we were happy to hear.

Another statistic, 55 percent delete any and all bank messages. So, financial institutions that I've met with have said things such as, well, one of the things we're considering is the nuclear option, just not using email to communicate with our users anymore, which doesn't make a whole lot of sense, given the fact that banks save an enormous amount of money by having people do their banking online.

So, not being able to, you know, communicate with them by email doesn't make a whole lot of sense, but, you know, you're heard -- and probably read -- Walt Mossbe enormous amount of money by having people 17 wial i555s

and 1999 when it was -- when it was all text? You know, we're seeing images being blocked regularly; links aren't working in emails, to a great extent today. You know, and advanced functionality is going to be blocked, because we can't trust it. It's a few bad apples that are ruining it for everyone else.

So, do we want email to be just for casual communications or do we want something more substantial in the industry? You know, there are those who believe, you know, right here in D.C., the U.S. Postal Service thinks there's a great market for putting the blue eagle icon right in email messages. Well, if images are being blocked, it's not going to work. Okay? Now they think there's a great market there; I believe it. We've partnered with a company called EPostmarks who believes the same thing.

There are, you know, state legislatures around the country who are thinking it may be a good idea to give email the same legal standing as first class mail. But, they need some assurances that, you know, that it's reliable, that it can be delivered and that that -- that blue eagle postmark can actually show up in the message.

So, what are we trying to do about it? Well, you know, taking us as an example, we are establishing a network of ISPs. We've got a number of relationships.

appear in inboxes in the list views, at AOL and YAHOO! and at others. And it will be the same across all participating ISPs.

When the message is opened, then you'll see it either in the preview pane or in the chrome of the message itself. Not in the body of the message, but in the chrome of the message. Again, a certified icon, this blue ribbon icon, along with, you know, a term indicating that it is, in fact, certified mail.

So, you know, our ISP partners have said, yeah, we'd really like to do this but only if there's a level of security that's appropriate under the circumstances. And, so, there are number of things that we've done. We've, you know, established a pretty thorough accreditation process, there are others in the industry who do this, as well. The basic idea is looking at a whole lot of senders who come to you and say, hey, I'd like to use that service, because I'd really like to get my, you know, my images working and my mail delivered.

Well, it turns out when you go out and say, we can do that for you, you get a lot of negative selections, so a lot of people who have horrible problems getting their mail through because they're doing, you know, bad deeds on the Internet, are those you have to reject. We have had to reject, you know,

most of the people who have applied.

(Laugher).

MR. HIRSCHMAN: As it turns out. You know, we do pick and choose. We go after some who we know are good mailers and, so, we do have, you know, at least a 28 percent acceptance rate.

At a very high level, the technology works by putting a -- it's very similar to Domain Keys in that we put a, you know, a digital signature in a header. There are some additional features, but it's not the same thing as domain fees in that we are actually putting a -- we are putting the signature within the -- the sender's message. So the sender communicates with us and says, hey, we'd like one of your tokens. We say, great, you know, if you pass the test, here it is.

What happens is then it's received by the ISP, the ISP looks at it and goes through a validation process, which includes, you know, validating the signature but, in addition, making sure that it's the right token on the right message through a couple of hashes that it runs.

So message tokenization is sort at the core of what we do. It allows to have certain control over the sender's actions in a couple of ways. It allows us to give out quotas. So, if a sender says, hey, I only send

advertisements from us.

So, again, the bottom line here is consumers have lost trust in the medium. We need to find a way to restore trust to them. There are a lot of technologies for doing so. We believe ISPs ought to buy into this idea of visual indicators of authenticity in the inbox as a way to signal the consumers that emails can be safe.

Thanks.

MS. CHRISS: Thanks. That was great, Ken, thank you.

(Applause).

MS. CHRISS: And on such short notice, too, that's pretty impressive.

So, Martha, come on down. TRUSTe. Also, a reputation service provider, but with a unique twist, I'd say.

MS. LANDESBERG: Well, hello, everyone. I am delighted to be here and I want to thank Sana and the Commission for inviting TRUSTe to be part of this.

Haven't we been hearing for days -- for yesterday and today -- and even on this panel, some of the most interesting and ingenious technological approaches to a terrible problem? I think it is -- we hear a lot about how smart the spammers are and how they

play the cat-and-mouse game, but the work of my colleagues on the panel here is just astounding, I

I'm going to talk to you very briefly today about our email privacy seal and the trusted download program. But for those of who have are -- who have been familiar over these past 10 years with the rectangular TRUSTe marks, we're still sticking with the green and black and white, but we've modernized, and I'm very excited about that.

So let me focus a little bit on the email privacy seal program. Oh, and let me mention, I do want to say that we are actively involved in authentication and anti-spam efforts and anti-spyware efforts, anti-phishing efforts, and a lot of our consumer education efforts are focused around that, and we help, in partner with a lot of other interested parties, in doing consumer education programs and materials that are all available on our website, and business education materials, as well.

And we are particular proud this year to have received the first AOTA award for nonprofit leadership in online safety. That's a really big deal and we're very excited about that. So, I want to talk a little bit about that.

So, onto our email privacy seal program very briefly here. This is a program that certifies email practices of websites. To earn this seal, which appears

Now, I want to give you a couple of examples of what -- and I should say that these -- there are key disclosures that appear on these pages where the seal appears, so that consumers know right away what the consequences are of providing an email address.

There's just a couple of examples. We require companies to say, look, what kinds of email -- okay, the consumer wants to know, if I give you my email address, what am I going to get? What kinds of emails? So, we have to describe, at the point of collection, what kind of email you can expect to receive, as well as whether the company shares email addresses or not.

So, you have to be very explicit about that, either way. And then the consumers have an opportunity, of course, to verify whether they're dealing with a TRUSTe licensee.

Now, we get complaints that come in through our watch dog dispute revolution process, which is linked from that verification page, and we handle those expeditiously, we work as an intermediary between the company and the consumer -- 99.9 percent of the complaints we receive across all our programs are resolved to both parties' satisfaction. We are very, very proud of that. And we service, as a backstop, really, for legislation and regulation, there's this

whole other piece where consumers can go right away, sort of -- almost in realtime, in effect, to get some recourse and get some assistance when they need it.

I'm going to give you my little pitch for why seals work. I'm going to give you a little sense of our

with a licensee in the email privacy sale program, or you're just kind of curious, you can click right through the verification page, and we tell you right there, if you're experiencing a problem with email from this website, you know, contact them, and if you don't like what you hear at the end of the day there, come to us and there are links right away to our complaint and dispute resolution system.

Now, I'd like to switch for a minute to tell you a little bit more about our trusted download program. And here we're -- I want to focus on the -- the -- some of the bad stuff that the emails we've been hearing about, you know, scams and schemes we've been hearing about, deliver or get you a link to deliver to you.

The trusted download program, we're very, very proud of. It is the first set of industry standards for downloadable software. We have been in beta for over a year now and we've published our first whitelist of certified downloadable software applications this past February.

Again, I won't read to you the key -- the key components, they're here for you to take a look at, but I just want to let you know, the way this works is, at the moment it is a back-end certification service, where companies submit their downloadable applications to us

for certification, and they have to step up to our standards, which include very meaningful notice at the point of download, prior to installation. For example -- I'm not going to pick on any particular kind of software -- but why is this application free? Because it comes with advertisements that have been -- that are going to be served. They are going to be pop-ups, they are going to be pop-unders, and those ads were brought to be by "X" software program. The -- we announce on our whitelist on the TRUSTe website, certified applications, and you can take a look at those there.

We think this is the beginning of a route to help marginalize the malware. If you get to a website where software is offered, you will have an opportunity to distinguish good from bad.

Now, initially, we're talking about portals and advertisers and ISPs and others who want to be able to check a whitelist and know, do I want to accept so and so's advertising in my system? Well, if they are using one of these software applications, I'm feeling pretty good about that.

We think some of the other marketing incentives that are really key is by making our standards transparent, software developers, who want to step up to this plate, are going to be making their own, you know,

they're going to be showing to advertisers the criteria they are meeting to make this work, and we hope and are beginning to see already that advertisers are making some of those business decisions to go with certified applications.

One of the other things that is most interesting, I think, from our perspective is that we impose very strict affiliate controls on companies that want to get certified. So that, as we all know, this notion of cascading trust that we've heard about, where there is a vendor who has a subcontractor whose subcontractors have their own affiliates, and you shoot your advertising out initially and you don't know exactly where it's going. Well, you can't get certified by the trusted download program if you do not have contractual controls on your affiliates that require them to comply with the trusted download program.

And one of the most interesting things we've begun to see is the shrinkage of these affiliate networks, because companies come to us and want to be certified and it's just not worth it to them to have these, you know, uncontrolled affiliates out there, because they want the certification.

So, this is just an example here of the kind of notice consumers will see at the point of download.

these things. It takes the tech protocols, it takes certification, authentication, enforcement, of course, and lots of consumer education and self-regulation to make this happen, and we're just very, very proud to be part of this mix, and I congratulate the Commission and my colleagues on the panel for all the good work all of us are doing to try to combat this problem.

Thanks very much.

(Applause).

MS. CHRISS: Thank you, Martha, that was great. That's great. Margot, last but not least, come on down. AOL's anti-spam manager for many, many years. Many of you may remember Margot from 2003, she had a simply riveting display of how to hack into, was it a Post --

MS. ROMARY: I think it was a Navy military server.

MS. CHRISS: Yeah. So, she's back this time to dazzle us. Thank you, Margot.

MS. ROMARY: All right. We have roughly 15 minutes until lunch time. The clock is ticking.

So, since this is keeping it out of the inbox, I thought I would do a brief walk down memory lane of where AOL has been, at the 50,000 foot level, technologically, for the past 10 years. And you're like, ah!, it will be really short, I promise.

our members to tell us immediately when they got a piece of spam and we could feed that back into our blocks and be far more effective.

In more assessment of the last ten years' worth of technology, this is the single most important thing we have done to get us out from behind the eight ball and really be there to counter-punch as soon as we saw a modification in spammer technology. I can't stress that enough.

Okay. So, then, what we started seeing was the nefarious activity, the really criminal activity, emerge. You had bad guys compromising end-user connections. This is the open-proxy problem. This is the compromise end-user service problem. You had real legitimate traffic coming with the exact same transmission and routing path as the spam.

So, point of origin was no longer viable. We had to do something contextual based on the reputation of what was actually in the message itself. And that's where we're at now.

You see represented by this pink bar, identification and reputation, this is sort of what my colleagues have been talking about, but in reality it represents thousands and thousands of servers looking at minutia in email.

I want to make a point here. We've talked about authentication and we've had lots of analogies about how really authentication is just -- are you or are you not who you say you are? And that's good, but that's not the whole picture.

And then we talked about reputation, we talked about sender reputation, and I want to say here that that's good, but that's not enough. You need to actually take reputation in the context of the message itself.

So, a sender, an IP address that has a good reputation for sending say, bank statements, because they're a bank, as soon as they start to send pharmacy stuff, that's a problem.

So, just because a sender is authenticated, has a good reputation, doesn't mean that all the mail is going to be sent -- well, it's going to be legitimate.

Particularly in this day and age of nefarious activity, hackers are hacking into legitimate sites in order to gain control of their email servers and send to us. I just want to make that clear. Okay.

So, this anti-spam technology evolution has been persisting since day one. We observe a problem, we identify exactly what we need to do to fix it, we mitigate the issue, and then the spammers adapt.

We've seen that over the last 10 years on the grand scale with each new iteration of our anti-spam technology, but it really also happens on the micro level every second. So, my point here, the first point that I want to make, is that service providers, mailbox providers, should not be forced to adopt the technology or flavor du jour of something that we think will stop spam in lieu of doing what we believe and we know to be right to protect our service and our mutual customers.

We shouldn't be forced to take the resources, since we are here, we are present, we know more, we know better than any other entity on the Internet what is causing our problems. We shouldn't be forced to take those resources and allocate them somewhere where we know they would get better used elsewhere. That's my first point.

My second point I already made, which is reputation is good. My colleagues have talked about it. Authentication is good, but you really need to take it in context of the actual message that is being sent. So, the reputation has to have lots and lots and lots of different components, body types, HTML, images, that sort of stuff. That's all. Thank you very much for the opportunity to come up and speak.

there.

But the challenge is as you look at the Fortune 500, we have to get beyond preaching to the choir. I think we're all -- many of us have been working with each other for years here, but it's really reaching out and to other business segments. We now have BITS, which is the financial services roundtable. They've now set a requirement, I believe, for the next 18 months, their members.

So, it's really getting out and really communicating the business value proposition to authentication and getting the right key stakeholders. I'll tell you at probably 95 percent confidence level

large corporation, requires a certain amount of diligence. They need to understand their own email sending practices much better than they probably do already. They need to understand all of the organizations in their corporation, maybe individual marketing groups, that contract with outside vendors in order to send messages, maybe a newsletter, maybe some support information to customers.

So, they have to do a certain amount of auditing. It isn't just a matter of publishing a record or starting to sign messages. You need to -- to go and understand your own email practices better than you already do, which is a good thing in any case.

MS. CHRISS: Mm-hmm.

MR. SPIEZLE: If I add to that, I think the challenges, these aren't technical challenges, but it's business processes challenges.

MR. FENTON: Right.

MR. SPIEZLE: And unlike other areas, it's not necessarily owned by one person. You can't go to these Fortune 500 companies and find the specific person that owns every outbound mail server. Quite often the work is out sourced, and so it is a process. And, so, those are the challenges we've learned.

MS. CHRISS: Okay, and it sounds like for large

corporations it's very complex in terms of the business structure, so as we move forward with this to make sure that the small businesses, Jim, you mentioned small businesses and micro online businesses, to make sure that they are in the loop, it would almost be easier for them in many ways, because they don't have those obstacles. And, so, we look forward to hearing about how we're reaching out to those groups, as well.

I'd like to move on to Des and Ken, who gave us great data about reputation services. I'm going to ask a tough question. How easy is it for a spammer to get a good reputation? Isn't it simply a matter of behaving for about six months, staying low and quiet, and then launching an attack?

MR. CAHILL: I guess the answer is directly related to how comprehensive is the reputation algorithm, how much data do you have, how vigilant are you in monitoring the message stream coming from that sender? And, most importantly, how quickly does the reputation system gather data about the sender's behavior and modify the reputation score.

In other words, a good reputation system is not a static score, just like your credit score is not a static score. You may have a great credit score, but then you may have, you know, go out and exceed your

credit limit and then ideally, the next day, if you're going out to then get a car loan, you're not going to be able to get that car loan. It's a sophisticated system that adjusts to itself.

So, any good reputation system is going to be taking complaints from Hotmail or AOL or other sources. If a -- if there's a bank that's sending out statements, and I expect to receive statements from that bank, and then all of a sudden I'm receiving Viagra emails from that bank or Nigerian oil scams, I'm going to hit the "this is spam" button pretty quickly, and a lot of other consumers are, as well.

So, I think the system is capable of detecting compromises to the system or a spammer trying to act like a good sender and then going bad.

MS. CHRISS: Okay, Ken, do you have any additional thoughts about that, the spammer's capability to use the reputation system in a bad way?

MR. HIRSCHMAN: Well, I would echo what Des said about how, you know, how it would catch up with them very quickly. And I kind of query whether the typical spammer or scammer is really willing to wait six months to --

MR. CAHILL: Agreed.

MR. HIRSCHMAN: -- you know, to launch an

attack. I think, I think, you know, they want to get in to your inbox much faster and much more reliably. And, so, I think some of the presentations we saw yesterday -- I think a very good one was one that Pat Peterson did showing you how, you know, very minor changes in content, in a message, can fool the hashes and can fool, you know, the image checkers. So, I don't think -- well, theoretically, yes, somebody could wait six months and then send a bunch of spam and then have to move to a new IP. I don't think that's as realistic as some of the other more sophisticated methods they're using today.

MR. CAHILL: Yeah, to echo what Ken says, bottom line is there are more cost -- unfortunately, there are more cost-effective ways for a spammer to achieve their ends.

MS. CHRISS: Okay. So, it's not that practical for spammers to do, and the reputation service companies, they're very flexible. They move quickly to get information from these spam buttons, to move quickly, so --

MR. CAHILL: Yeah, it's not just a one-time event. It's ongoing compliance and monitoring.

MS. CHRISS: Mm-hmm. That's good to know. That's good to know.

with the understanding that sometimes we just can't help if we are not allowed to say who's got the problem.

But sometimes the complaints are -- do raise a systemic issue. And we do regularly report statistics on our complaints to the Department of Commerce, to the Federal Trade Commission, you know, anyone who asks. And our own enforcement activities are all published on our website.

MS. CHRISS: Terrific. That's good to know. That's good to know.

Margot, I have a question for you, and I think you really got to the outer edges in your presentation about why is it that we are not seeing ISPs on a wide scale negatively scoring unauthenticated email or taking certain action against unauthenticated email. Tell us more about that.

MS. ROMARY: Well, you can sort of sum it up, I think, with something that perhaps Richard said about how --

MS. CHRISS: Maybe Ken?

MS. ROMARY: Oh, no, it was something that Richard said about how a vast majority of the authentication, SPF, DKIM records are misconfigured for sending entities. And to --

MR. FENTON: Des.

MS. ROMARY: Des? Was it Des?

MR. FENTON: Not Richard.

MS. ROMARY: Sorry.

MR. CAHILL: That's okay.

MS. ROMARY: To require a receiving organization to adopt email refuse or email accept standards for organizations where there's no governing body that makes sure that the stuff is correctly implemented, I think is a big mistake. Many organizations, like some of my esteemed colleagues here also mentioned, don't even have all of their servers published under their records, so we would be excluding a good deal of legitimate email potentially if we did refuse.

Additionally, there's such a high chance that you could have DNS failures, you could have technical glitches that even for three hours' worth of time could impact the legitimate traffic of email that I think it's a mistake to force organizations to adopt how one treats email that's authenticated.

MS. CHRISS: So, it's too early, Margot?

MS. ROMARY: Yes.

MS. CHRISS: Just too early?

MS. ROMARY: It is too early.

MS. CHRISS: Okay, that's fair. That's fair enough. One more question for Margot, and I'm over the time, and I do want to open it up to the audience a little bit before lunch, so I'm going to apologize, but just one more question from me.

Margot, you said it, you said as an ISP, you guys have this panoramic view of what's going on, you can see it all and digest it all. I know that that spam button that you introduced in 2003 was really great in terms of hearing from your customers, but when it comes to spambots, to somebody's computer being turned into this robot, most times the customer or the consumer won't even know. So, tell me how you are -- or how ISPs are uniquely situated to stop and cut off spambot activity.

MR. ROMARY: We happen to be in the fortunate position that we own a network, an access network, or ATDN network, which we lease to other providers, as well, so we can see traffic, bit torrents, we can see compromises as they're occurring, as the zombie, the drone machines, end-user connections are trying to phone home to their master DNS servers or whatever. And we're able to very, very quickly shut those down.

I think -- I wanted to have one of our security folks come and do a demonstration on what we're calling the fast flux proxy network, but he was too afraid for

his own personal safety. He thought the bad guys would come and knock down his door and beat him up, so it was noticed already, months ago, that AOL's ATDN customers were not participating in these fast flux proxy networks, because we, under the covers as security folks, were disabling them, disconnecting them from these networks.

So, ISPs, AOL particularly, is in a very advantageous position that we can find the bots as they get infected and stop them from participating in the networks.

MS. CHRISS: Well, great. That's great. And hopefully we'll see more of that bot-stopping activity down the road. Quickly, right before lunch, do any of you have any questions for these wonderful -- lots, lots of questions. And I have question cards, as well. The gentleman in the orange shirt first, please.

MR. LEIBA: Barry Leiba. Martha, I have a question for you about the TRUSTe seal. It seems to me that you've taught people to look at the content of a web page that may contain a graphic that looks like a TRUSTe seal and to believe that. And that doesn't seem necessarily to be a good thing. Can you comment on that?

MS. LANDESBERG: Can you explain a little more about why you think --

MR. LEIBA: It's very easy. I can put something that looks like your seal on my webpage and ask people for personal information, and according to your presentation, 70 percent of the people that you've surveyed think that that makes me more trustworthy. Now, sure, ultimately they can complain to you and you can chase me down, but in the meantime, I may have done a lot of damage.

MS. LANDESBERG: Yeah, I mean, I think -- well, one answer is that nothing is completely bad-guy-proof. We think, though, that the verification path method that we've chosen, which is that you can click through that seal and either find something or nothing. It makes it a little more difficult for the spoofer, but again, I'm not -- you know, we -- I guess there are two sides to the coin, and as I mentioned earlier, we're finding that we have a lot of interactions with consumers around. They can tell.

MS. CHRISS: And it is a layered approach, Martha and a lot of the other panelists mentioned, that a lot of these things on their own are spoofable, if you will, but with a layered approach, it just makes it more difficult, if I may chime in.

Okay, I have these wonderful question cards, and I'm going to invite people to come up to ask the

panelists these questions. A lot of them are kind of company-specific, in any event, so please do that. I'm going to close my panel now and just congratulate everyone on these technological tools that we have to manage this problem. Thank you. Thank you very much.

(Applause.)

PUTTING CONSUMERS BACK IN CONTROL

MS. YODAIKEN: We'll go ahead and start. We're waiting for a few minutes because the last panel ended a bit late. But we'll go ahead and start now. You're here for the Consumer and Business Empowerment Panel, and what we are going to talk about is how to have ways to empower consumers and businesses in their role.

Yesterday, we heard a lot about cyber criminals and fraudsters trying to use email to bring malicious code into computers and into email servers for businesses and we heard about the different ways they do that in terms of sending emails that contain these things in attachments or that get the consumer to do something that helps get the code into their machine, whether that's go to, click on a link or take some other action of downloading something.

We heard that these do two things, mainly. They damage the computer systems and they take information from them and they work to trick consumers into more elaborate phishing initiatives. But they also compromise these computers, whether they're the individual computer or the server, they compromise these computers and try to make them part of a network that's used by cyber criminals and by fraudsters to perpetuate more crimes and frauds.

Reports, which is published by Consumers Union, and he's going to talk to us about new data that Consumer Reports has gathered in terms of analyzing these tools that are out there for consumers to protect themselves.

And we have Miles Libby, Senior Product Manager at Yahoo!, who is also one of the co-authors, Domain Keys, Identified Mail, which was discussed earlier, and Miles is going to talk to us about email service providers and how they try to help consumers, what they do to work with consumers so that consumers are aware of what's going on and can try to have better habits and help those around them.

Okay, Linda?

MS. SHERRY: Thank you, Ruth, and thanks to the FTC and Chairman Majoras for holding this important Spam Summit.

So, today, I'm going to talk a little bit about some of the challenges that face consumers in trying to identify spam and malware, which are significant we believe. The first of which is complexity. These protective programs really require a very high level of expertise in some cases just to purchase, download, install and to run effectively and to update effectively, and we find little evidence of standardization among the different software companies. It seems like many of the

companies have taken their own path in this, in developing these products.

There is substantial cost in protecting yourself from spam. First of all, when you purchase a computer, many people think perhaps that the protection should be built in to the computer from a lot of these things, but software costs money. There are free options out there, but I think, somehow, consumers don't necessarily know about them. And there aren't a lot actually as I look out online. And consumers may really miss genuine opportunities to receive mail.

As one example I like to use, we send out advocacy emails to people who have actually opted in, and very often, it will get in their junk mail or they will email me back saying, well, because we haven't emailed them and we don't email a lot, so they'd say, you know, I don't know you. Well, you knew me six months ago when you signed up, you know. So, this kind of thing is very difficult, and, so, we can't get our message out.

There's costs involved if the fraud or malware damages your computer or you click on a phishing email and you get -- or lottery type of fraud. So, there's costs that way, too. And we really wonder -- we think everybody, all the players have to think about is it to make consumers responsible for all these additional

costs.

The frustration of dealing with spam. To protect yourself it takes a lot of time and effort and just because spam stays out of your inbox doesn't mean you don't have to do something with it. You have to deal with it later in the junk box or perhaps you have to backtrack with colleagues and other people to make sure that, for some reason, their email didn't reach you, if they emailed from home or that kind of thing.

A lot of people just give up, which is not good for the system. Email holds a lot of promise. It's already shown us many of its promises for communication purposes in the future, and we don't want people to give up.

Computer performance, one of my favorite points, and on some computers, when you're running the security software, the anti-spam software, the anti-virus software, it slows that computer down, and nothing really -- you can search on -- you know, you can Google, you can search on the Internet, if you're savvy, and a lot of it still won't tell you why it's doing that.

The frequent updates will kind of stop you in your tracks when you're trying to work. The scans going on will slow things down. We find that consumers will just maybe turn them off which, of course, is a terrible

thing to do because then they're unprotected.

The onus is, unfortunately, now on consumers to protect themselves. I don't really think that's fair, and I'll say something else about that in a minute, but recognizing phishing and other social engineering tricks, we're leaving that up to the consumer at this point. We're saying, you know, a phishing email looks like this, don't click on it, it's from your bank.

Find misdirected legitimate emails. That can be tough because somebody will say to you -- your boss will say, I sent you that email. Oh, well, I never got it. You know, you feel so silly.

To mark spam, that can even be a challenge. I mean, you might mark something -- for some reason, Chico's has targeted me with -- I guess I checked the wrong box or something. So, you know, they are -- I feel they're spamming me even though they're a company I go to to buy clothing from.

You have to check the junk mail box. You have to read and understand the consumer education materials that come from providers or are on the online help.

Now, that's a significant time -- dedication of time, which many consumers don't have today. And some of it's written in such terms that the consumers themselves can't possibly understand it either.

You have to be able to determine who are the trusted entities out there that I really want to do business with, you know. Do I want an advocacy email from Consumer Action? Did I sign up for an FTC newsletter? You know, this kind of thing. You've got to remember all these things. And after a couple years go by, it can be a little hard.

Navigating all of the marketing and privacy options that are out there, I mean, how many of us really take the time to look closely at the privacy statement, even in this community of very knowledgeable folks. Sometimes we just let that slip, you know. Sometimes when we're buying something, we don't notice that the default's set to the check, that we could get their emails, just because we're engaged in a process and we don't really think about that.

It can be a real challenge to tell the difference between spam and legitimate email. If legitimate emails come too often, you know, they can seem like spam.

Deception and fraud. Fraud is really tough to tell sometimes because they have thought overtime about tricking you. That's where the social engineering comes in. They've got -- you know, they've got your -- they know what buttons to push.

These take-over email accounts, how do you know it's not coming from the person that -- you know, Consumer Action, they took over our server once, people were yelling at us, you know.

Sneaky graphics and links. Your boss sends you, again, a word file, you click on it, you don't think twice. Somebody else sends you an attachment or a little movie that they say is funny and you maybe don't think twice and it's malware.

What about unknown senders who might have something you're interested in? What if we want to tell you that you need to act today to help a really good law pass? But if you don't remember us or you don't recognize the way we're sending you email, you may ignore a legitimate opportunity to make a difference.

Aggressive marketing, which I already mentioned, some companies just don't seem to get it that people don't want to hear from you every day of the week.

There's a technology divide and an overload for consumers, whether they have PCs, Windows PCs versus Macs, turning on firewalls and setting security choices in the computer, very complex business. OnGuard Online does some great education in that regard.

Making warnings and updates meaningful. This is very important. Some of those updates that pop up,

they'll say, is not a real domain name. Well, my brokerage -- I just clicked on my brokerage the other day and up came, is not a real domain name. Well, I've gone there a hundred times and I know it is. But if I was an unsophisticated person, what would I think, you know?

There are all these different browsers out there that people use. Well, not all these different, but several main browsers. They have different capabilities. You have to set the settings in a different way. You find them in almost a different place, the preferences. Just imagine trying to tell your mom how to set the preferences on her browser. I mean, you may have sophisticated moms, but mine is like, aahh, you know.

Unsubscribing versus spam reporting, should you click that button to unsubscribe? Should you report it as spam? It's just a big question. And there's -- a lot of people don't understand that when you give your email

to come and listen to your products, you know? Find out what your products are, vetting your products in advance, helping support that time that consumer staff -- organization staff member is taking to come and do --

that do marketing. I mean, to have the box checked to receive emails, et cetera, that's just -- it just doesn't make any sense. You want to always do it at the most lowest common denominator.

And, please, please, please, do not blame the consumer for not -- failing to protect themselves. It is extremely important that we realize that this is complex. You're all -- a lot of you work for technology companies -- and consumers are just not equipped. They don't have the background you do; they haven't been looking at this every day of their lives since 1995 or before. And, so, let's don't blame them. Let's help them get where they need to be to avoid it and to help us all refine and make sure that the future of email is strong and helpful to everyone. Thank you.

(Applause.)

MS. YODAIKEN: Thank you very much. You want to go ahead, Dave?

MR. LEWIS: Well, I'd like to add my thanksaad, Dave?

not, at this point, in a position to fulfill its potential. And that's partly what I want to talk about, and of course how do we keep from killing them off, intentionally or unintentionally. And it's really the unintentional shackling of the killer app, the actions or inactions that we may take in the name of the consumer and the name of email security that concern me and the

something that a survey that we conducted, along with MarketingSherpa, that found that consumers felt that email was more useful than postal mail and particularly among the younger age group, 18 to 34, it's more useful than phone, though not as much. Nobody wants to take away the cell phone from the younger set.

Most importantly, it's the best way to receive service notices, bills, account statements, by 41 percent. And, you know, when you think about what we've heard in terms of the phishing attacks and such, you know, 41 percent is a pretty good number in light of all those kinds of malicious use of the medium.

And I think the really key statistic here is that consumers felt that it was the best way for companies to communicate with them, for the companies that they do business, to communicate with them, 64 percent, 72 for the 18 to 34-year-old age group.

And when we look at the business view of email today, when I was in London a couple of weeks ago, some stats that hit me there, I think I'd like to know the U.S. equivalent, about 50 percent of the communications -- personal communications are now done via email, about 70 percent in the U.K. on business-to-business, which is a pretty alarming stat.

Obviously, marketers are hooked on email. We

know that; 95 percent of them use it for some very unique benefits. The DMA published some stats about the contribution of email, which when you look at its economic contribution, is significant; and particularly when you look at the ROI, and that's, of course, what businesses are looking at in terms of what medium they choose to use to communicate with their customers.

But I think you need to look beyond the marketing applications and look at how companies are also using email for non-marketing things, in terms of getting service notices and statements and things like that out to their customers. And it's how all of us transact business with partners and suppliers and everyone else.

And I think at the end of the day, you know, the medium absolutely has the potential to displace the USPS, and God knows, with some of the postal rate increases and such that we've recently seen, businesses need an alternative to the USPS.

And, of course, email is also -- is what really holds together e-commerce. Without it, you wouldn't have the ability to conduct e-commerce on the Internet. And I think lastly, many companies are now fully dependent on email. They've optimized their operations around it. They simply can't revert back.

So, my point is that email is business-

critical. So, why then is the killer app a shackled prisoner? I think that because these adoption stats, despite the contribution that email is now making, it's a

and I think Trevor Hughes from the ESPC alluded to this in his opening remarks yesterday, is that the killer app is under assault not just from spam and the abusive practices of criminal elements, but also the measures being taken to combat those elements. So, what will kill it is its own failings.

And I think the risks come in two fundamental areas that our failure to solve the problem through self-regulation will invite government intervention. Hope not, but that's a risk. And our failure to find the right balance between security, protecting consumers and the legitimate uses of email ultimately impairs the medium for communication and commerce. And but what I personally believe is that we're very close, dangerously close, to both of those potential options.

So, what I'd like to really talk about is the ways in which we keep the killer app off of Death Row, and that really gets to something that this panel is all about, and that's empowering the consumer in my mind. There are two potential ways of preventing that outcome. One, I think, is to inject some new thinking into this debate; second is to engage all the shareholders in the ecosystem, and that includes consumers, in a way that really preserves and protects it. And I think we, as part of that, need to redefine the roles that each of us

spam. I see it as there's really two classes. There's the evil, which is the stuff that is dangerous and criminal and doesn't conform to regulation and makes every attempt to evade detection. And there is the stuff that is bad, email that doesn't -- that does conform to regulation, may well be authenticated, but simply doesn't recognize good practices and is email's equivalent to

r88tv 1.00004000 cm0.00 0.0n88ttices and is email's equivalent to

role. And what we did find is that 53 percent want to have trust tokens, they need that to be able to make further determinations and decisions around what's safe

they've even taken some of it. This presentation, I'm going to mention, there is new material. If you didn't see it, there are copies on the table, and also if any media want to use any of this information, there's a media contact on the sheet, if anybody wants to use it.

So, this is a little unusual because this summit is being held three weeks before we publish our annual cover story and package on this whole subject, so it came at kind of a little bit of an awkward time for us, but we decided to release some information from the September issue, which doesn't come out for a few more weeks, incorporated into my presentation, which is somewhat a break with our usual practice in order to help the Commission.

As you can see, I grabbed your logo. I'm going to just give you a very quick background on our involvement in cyberspace in the last few years. Starting about five years ago, Consumer Reports in addition to the TV and car testing that everybody knows and loves, began testing protection software, first anti-virus, then anti-spam, and more recently anti-spyware. Now we test them all every year.

Three years ago -- seeing that there was -- there was really no independent source of national data about the impact and costs of these various gorges that

we've been listening to since yesterday, we undertook the job of actually doing that ourselves and presenting it on an annual basis. So, these are kind of like, you know, annual benchmarks.

We do our state-of-the-net every year, in our September issue. This is a nationally representative sample. This was last year's, and as you can see, some of the major problems here totaled more than $8 billion in losses to consumers, both in repairs -- I think in one case, a million consumers had to actually throw their computer out, prompted by viruses and spyware infections. So, you know, we talk about losses to bank accounts and these pump-and-dump scams, but there is other losses besides what we've heard the last couple of days.

As I said, the 2007 version of this will be coming out shortly. The following trends that I'm going to present do incorporate the 2007 data, as well as the data from the past surveys. So, a couple of key questions that we're able to address in the data here are consumers receiving more or less spam these days and how is software holding its own. And that's not from the survey, that's from our tests.

So, on the one hand, in terms of, you know, we've seen all this data about the actual rise and volume, it's 99 or 90-plus percent of the volume out

there, just a tremendous amount of spam circulating around, but over the four years that we've been conducting our survey, the number of people that say that they're getting a lot of survey -- I'm sorry -- a lot of spam has been dropping. And we attribute that both to improved practices by consumers, as well as, you know, better filtering by Internet providers.

This is the one finding in this presentation that doesn't come from a survey. This is a summary of our spam-blocking tests over the last five years. We started it five years -- well, this is our fifth year. These are the number of email programs we test and the number that were like high passes that excelled in certain categories of recognizing spam and also recognizing legitimate mail.

As we can see over the first few years, there was -- if you look in the column on the right, which are the products most people buy, you know, the add-on spam-blockers that you use with your email program, four years ago one out of nine was a high pass. It's been improving up to last year. From last year to this year, we see a little bit of a drop back. Again, this is based on ratings that have not been published yet, so I can't give you the names of the products. You'll have to wait another three weeks for that. But as you can see, it

looks like the -- you know, the anti-spam products, this is an arms race and they may be losing ground.

Some other results from our four-year analysis, there's some good news and there's some bad news. Good news, consumers are getting smarter about protecting their emails and their computers. For example, fewer are clicking on the links in spam. You know, I heard a complaint yesterday, I think it was from a marketer about, you know, clicking unsubscribe is, you know, that's old hat, you know, that's old-fashioned, that's like superstitious, you know. These days you can trust mail.

But, in fact, there's nothing to stop a phisher, for example, from sending, you know, a routine looking mailing and when you click on the unsubscribe link, sending you to like a website with a drive-by download. So, you know, I, for the most part, do not click on those unless I'm absolutely, 100-percent certain where it's coming from.

Also, fewer consumers are replying to spam, again, trying to stop spam by replying to it. I think these are responses to all the education that the FTC and us and a lot of other parties have been doing the last few years, educating people about managing. More people are using a spam blocker. Now we're up to about almost

two-thirds of people that are using spam, you know, spam-blocking on their home computer.

And we're seeing an increased use of firewalls, also, over a few years ago. However, we're still -- there's still millions of broadband users who aren't using firewalls. It's not 100 percent there, and our calculation is, broadband users who are very vulnerable to hackers, there's still a significant number, in the millions, who are not using firewalls. So, this is good, but the job there is definitely not done.

Now, some of the bad news. Many consumers are still engaging in behaviors that help the bad guys. I know these little green bars look small, but if you look at the note under it here, because we use a base of around 78 million Internet households, even that little green bar still represents a half a million consumers that are admitting in our national survey that they patronize -- you know, they've bought a product or service based on a spam.

You know, so you can see, you know, that's where the money -- some of the money is coming from to fuel these things. Although you've seen it has gone down, but it's still significant. And this is very important. Despite all the savvy that we saw in the earlier graphs about people not replying and not clicking

on links, this is 8 percent of all the Internet households, not 8 percent of people that receive phishing, but 8 percent of all people, period, gave information to a phishing-style email. That's huge, and that, you know, suggests that people need -- we need more education in that area.

So, here are some recommendations. They're directed to the different stakeholders in this situation. So, really, this is to everyone. The survey results show that education over the last few years is working, slowly. To change the behavior of millions of people is a slow process. It's working, but I think we should build on it.

And based on that, response rate for phishing scams clearly we need to put phishing scams front and center now in education campaigns and push that up more. I think most people are pretty familiar with the click-on link issues.

Other suggested ideas for -- I personally don't see a presence of this kind of education in the places that my family and my friends frequent. They don't go -- unfortunately, most of them don't know about OnGuard Online. And I think we need to be in schools; we need to be in computer stores; I could see public service announcements, you know, like the anti-drug and other

type things. I think we need to step it up and make people a lot more conscious of this stuff. I think we even need perhaps to, you know, find some way to incentify people to keep their protective software up-to-date, because a lot of people just don't know that, you know, if you don't renew the contract it becomes relatively useless.

To Congress, some suggestions for making CAN-SPAM work more for consumers. I think in light of all the crime, we're not, you know, talking that much about, you know, what they've talked about, you know, the bad guys who aren't actually criminals. But we don't consider, you know, opt-out to be empowerment. That's what CAN-SPAM specifies, and in a sense, it legitimized spammers, because people can send you stuff until you make them stop.

Yesterday, Rick Lane, I think, of News Corp. suggested civil penalties for spammers. We -- you know, we're suggesting something even a little more ambitious, which is to establish a private right-of-action on spam, similar to the junk fax law. It's been obvious, you know, from these presentations, the bad guys way outnumber the good guys, and it's really time to start, you know, beefing up our side. I just don't think we're going to get all that money for law enforcement.

this later, the OnGuard OnLine, which both Jeff and Linda referred to, is the website www.onguardonline.gov, and that's a collaborative effort that the FTC has worked on with other entities to try to put good consumer information out there.

MR. LIBBEY: So, hi, I'm Miles Libbey. I'm the anti-spam product manager for Yahoo! Mail. So, I'm going to talk to you about how we try to empower our consumers through the products that we build and how we -- that our approaches into our anti-spam systems.

So, we host a wide variety of consumers across the world. ComScore claims that we have more users, not only in the U.S., but also throughout the entire world. So, that means we have users like Linda's mom to the, you know, absolute techno-geeks in China and Korea and everywhere. So, we host ISP mail from, for instance, AT&T and British Telecomm.

And I think, so, one of the reasons why we've had that market success is because we take a very consumer-centric approach to spam. And, operationally, we define spam as whatever consumers do not want in their inbox. And, so, every morning when I wake up, one of the very first things I do after getting my kids some breakfast is go check those -- that spam metric and say, you know, number of messages that a user sees in their

inbox that they consider to be spam. And we track that on a daily basis.

And, so, we've been using this number -- these number of messages, market spam, from senders as a primary spam-catching technique for a very long time. This is kind of the reputation systems that folks have been talking about all afternoon. And, so, we frequently find a very high agreement amongst the community, but sometimes there is -- you can see different groups of people disagree with what the community thinks is spam.

For instance, Linda was talking just a moment ago about her experience with the Chico mail, so perhaps most users might think that the mail that they receive from Chico is fine, but Linda happens to disagree. So, anytime that Linda would mark that message as spam, then we try to actually create filters in the background just for her so that the mail from Chico will arrive in her spam folder ongoing, but, for instance, my wife receives that mail and she wants to receive it in her box, she can do so. And we do that all behind the scenes without

positives. So, we typically try to deliver all of the spam that we get, except for the most malicious kinds, and we'll tag that and put it into the user spam or junk folder. And that way, if the user does have a chance to see or does -- we do have a false positive, we see that the consumer can actually go find that message, report it as not spam, and we can either, again, override the community decision for that user or update the entire community's view of the sender's reputation.

So, in addition to the behind-the-scenes features that we do, we were able to spend a lot of time on developing some user-facing anti-spam catchers, so actually a user can go and interact with. So, I won't go and talk about all of these, but one of my favorites is a product we called AddressGuard, which has a disposable address feature. So, the idea is that you can create up to 500 different email addresses.

And as you're transacting online or surfing whatever, you can make an address, give it out to that person, and then if they -- if that address starts to attract spam, then you can simply throw it away, never to be bothered with it again. So, we think that this is a really powerful tool that consumers can use to help themselves -- or proactively help themselves and keep their inbox free of clutter.

So, one of the other things we've seen over the last couple of years is the web has spent a lot of time focusing on how a -- how they or the companies can prove

around here. Margot before mentioned that she thought that this spam button was the most useful technology invented in a long time. I agree with her. It's one of those things we think is an immensely valuable feedback for us, and I certainly encourage all consumers to use that button and let us figure out that -- or use that wisdom to its most advantage.

MS. YODAIKEN: Thank you very much. Thank you, Miles.

(Applause.)

MS. YODAIKEN: Okay. We've talked about a bunch of things up here, so let's start on the issue that you raised, Linda, and that you've all kind of talked about to different degrees, which is we talked about the responsibility of the consumer versus the burden on the consumer. Linda, you talked a bit about how it's a lot for consumers to go and read the information they need to know or to update their anti-virus software.

And, Dave, you talked about how the consumer is really sophisticated and could actually give a lot of feedback in terms of not just this is -- you know, not just this is spam, but a little bit more in terms of, well, really it's not spam, it's just that catalog that I just don't want to see right now, and I'm trying to get it out of my inbox.

So, can you all talk -- Linda, you want to start? I'll start with you, and maybe we'll walk down and see who wants to talk about the burden versus responsibility.

MS. SHERRY: Yeah, well, I've talked to various people. I kind of have my touchstones, not only my mother, but other people that aren't very technologically savvy, and I've talked to them about, for instance, filtering emails. They have no idea what that is really, a lot of them. So, for instance, if I wanted to make sure all my Chico's things go into one Chico's folder, I can do that. And then I can look at it or not look it or erase them all at one fell swoop.

But for some reason, these kinds of very basic messages about the tools that are out there are not reaching consumers. Now, I think that perhaps you've got -- these are captive consumers. These are your customers. Either they own one of your computers, or they use your ISP. And I'm just thinking that can't you build in sort of reports, you know how American Express gives you at the end of the year, would line up everything you've spent in different categories and give you this lovely report. Well, couldn't you do this periodically with consumers?

So, instead of some pointless little popup box

actually is popping up a really useful, maybe PDF or, you know, they could click on it or something, report that would basically say to them, or give these people information, these consumers information about what are they actually doing online. For instance, I mean, your firewall is set at off. You never -- you have not reported any spam messages this quarter. You know, the following authenticated senders have sent you email this quarter. Give their names, authenticated by, give the little -- give the URL where they could go and see these authentication companies.

You have received email from the following unauthenticated mailers this year. Let's empower consumers with information that they can really use that's -- and not too long and involved, but something that they can actually kind of at a glance look at and learn to expect and learn to look for periodically and to use the information that's in it.

MS. YODAIKEN: Okay, so to create a dialog, Dave, does that kind of work a little bit with some of the stuff that we had talked about?

MR. LEWIS: Well, it does. The point I was trying to make, relative to consumer empowerment, is I think we've had a certain mindset around what the consumer needs and wants. And at least with the ESPC

survey, we're beginning to challenge some of those underlying preconceived notions. And I think the behavior of consumers at domains like Yahoo! and AOL and the use of the spam button and what I talked about in terms of their desire to have additional tools at their disposal, and those can certainly extend to summary tools and things of that nature that would allow them to better manage that inbox, there's a high percentage of consumers that are willing to not only -- that they're able to use those tools but also willing to use those tools.

To your question about, you know, I think your question about, you know, what is the responsibility of the consumer when it comes to these things, I think we should recognize the limitations of technology. And that's partly what I'm saying here, is that even from a high-tech company, I'm saying that, that we need to hear that consumer voice more directly and in a less ambiguous way.

And my belief is that if that voice comes through, what we now see as bad mail, not the evil stuff, that if those senders, those marketers run the risk of being blocked from the medium that their customers prefer, you -- and they know why they're being blocked by that consumer. And there may be more -- frankly, those consumers may be more exacting than the ISPs themselves.

You will affect behavior change. So, that's my point.

MS. YODAIKEN: Let me just ask a little follow-up question on that before I get to everybody else. So, on that, in terms of -- aren't there already ways, I mean, in terms of if you're -- if a business' email is being blocked, isn't that because a lot of consumers have reported it as spam --

MR. LEWIS: Not always. Not always. And that's part of the problem. In many ways, these filters are based on panels, they're based on more blunter instruments, like content that's, you know, been coopted by spammers, so legitimate marketers use it and find their mail is intercepted and routed to the spam or junk folder.

So, no, the filters that are being used and that affect legitimate business are based on more than just what the consumer has to say, and that's partly my point, is figure out what's malicious, let the ISPs deal with that. But empower the consumers with the tools so that they can more effectively manage those things themselves.

MS. YODAIKEN: Jeff, you want to jump in?

MR. FOX: Yes. I think this speaks to the relationship between the consumer and the ISP. I mean, the consumer is the customer. They're paying the ISP to

deliver, and I think the ISPs know who they're -- you know, where their money is coming in from, where your paycheck comes from. And, so, I would think that it would behoove the ISPs themselves if they haven't -- I don't know if you've done it, to find out from their customers if this is what they want, because I don't think that the ISPs are there primarily to serve the senders; I think they're there to -- who aren't paying them -- they're there to serve the receivers. But if the receivers are not being well served by the current system, the ISPs should -- you know, the normal market should work.

MS. YODAIKEN: Okay, Miles?

MR. LIBBEY: Yeah. I mean, I think it's -- from our point of view, we need to make sure we're providing the best user experience possible, so that means delivering the messages that the users do want in their inbox and they don't want into their spam or junk folder or not at all. So, and you can use that feedback mechanism to help us say, you know, I really do want that Chico's mail in my inbox or what have you and then kind of retip the balance, if you will.

MS. YODAIKEN: Let me do a little follow-up on that. In terms of the kind of -- so, we know, you're working really hard and you're blocking -- you got a lot

of stuff that's coming in, directed at the consumers, and you're blocking as much of it as you can that's bad, and you rely on some consumer interaction. And when you get those important, you know, clicks from consumers to say this is spam, that helps you make your decisions about how to go forward, and there's a relationship there. Is there any need for a relationship that goes further back, where you're contacting the businesses and giving them what I seem to be hearing from Dave is a little more feedback on, you know, what's happening?

MR. LIBBEY: I mean, I think there's been a lot of collaboration efforts in the last several years, with the ISPs and the senders. Over the last, say, 18 months, I think, a lot of ISPs have started to begin to use feedback loops. And MAAWG has spent a lot -- a fair amount of time working on a way to standardize that feedback, called abuse reporting feedback protocol. So, and more and more ISPs are starting to use that to be able to send those -- the spam complaints back to the sender.

MS. YODAIKEN: Okay. Let's talk about -- Jeff, I wanted to jump in and ask you a question. You had done a little work on some of the protective measures that consumers have in terms of not just how they respond to email, but how they try to keep their anti-virus software

going and so forth like that. Do you want to talk -- can you tell us a little bit about some of those choices that consumers need to make and some of the factors they need to consider?

MR. FOX: Yes. And I spoke with our engineer who's been testing, you know, the software for years. One is that -- he said that, you know, a lot of consumers don't know that if they don't renew, you know, the annual fees, that the thing becomes, you know, eventually ineffective, and many people are used to buying a word processor, which is basically good forever.

Another thing he suggested, because there are compatibility issues and conflicts between differing products, is at this point it's probably best for the consumer to go for a suite and use the firewall from the suite rather than the operating system, because not only is it simpler, but it pretty much guarantees everything will work together in a nice way.

You know, he had seen some cases where even one manufacturer themselves wouldn't allow their anti-virus and their anti-spyware software to operate side-by-side as independent products. If you wanted both of those functions, you had to uninstall each of their products and then get their suite. And in this case, they actually were willing to send their suite as a

replacement for free, but it was kind of odd that even with the same manufacturer the products wouldn't work together. You know, a number of other problems, the question about using two anti-spyware or anti-viruses, there are ways to use these things together, but you have to know, which most people don't.

MS. YODAIKEN: Okay, so let me ask anyone who wants to jump in. Miles, I'm sure you -- I thought of you because you guys actually actively try to get your customers to update their anti-virus and to use anti-virus software. How does the consumer really know what they should be doing? Who should they turn to in terms of trying to figure out what protective measures they should be taking to protect themselves?

MR. LIBBEY: I kind of think this is one of those responsibilities that the entire industry shares, so whether it be the media, whether it be the FTC, whether it be either the ISP or mail client, I think we all have a role to play in helping to educate consumers about what they should be doing and what they shouldn't be doing.

MR. LEWIS: Yeah, I would agree with that completely. It is a shared responsibility, but you need to be balancing that as you balance, you know, the security versus commerce issue. You need to be balancing

you're in a business situation, the staff might say, well, our technology department is going to take care of that, so their habits in terms of email use and surfing and so forth was different, so --

MR. LEWIS: Well, you know, I think all of us are in all three roles, in my mind. There isn't a sender, receiver, consumer role that any of us play. We're all kind of in all three camps, in most instances. I think the biggest challenge we face, and authentication is a good example, is on both the receiving side and the sending side, when you get down to, you know, the smaller entities, it's extremely tough, okay?

So, you know, we've got to maybe create some business opportunities around taking it to the lower end of the market, where the fat part of the pyramid is and where the bigger risk is, in terms of finding ways in which to allow those things to be implemented, because our company, for example, I mean, we authenticate outbound email, but we're not as careful on the inbound.

And, so, what does that permit to have happen? Things to sneak into our corporate environment, and, you know, inadvertently access, you know, critical data. And the same is true with a lot of companies. You see the compliance more on the outbound sending of email than you do on the inbound. And we need to kind of look at it on

both sides.

MS. YODAIKEN: Anyone want to add anything on that? Miles, do you have any thoughts?

MR. LIBBEY: Sure. I mean, certainly I would recommend for businesses to go ahead and authenticate your mail, certainly take advantage of all the feedback loops that are available through the ISPs. You know, every time that a business sends an email, they're putting their reputation on the line, whether they know it or not.

And, so, the feedback loops are a great way to start to get an understanding of how consumers view their mail and how they can take both reactive and proactive measures to protect that reputation. And there's lots of infrastructure hygiene kind of situations that you have, but that would be a whole different panel, I think.

MS. YODAIKEN: Jeff, go ahead.

MR. FOX: Yeah, I would say, like everyone

that's really going to be a problem for your staff.

MS. YODAIKEN: Linda, you had also talked about

know, are more and more set at a very high setting, and if you want to play around with this, these are the things that you should look at?

MS. SHERRY: I think we have to set them at the highest protective level, because what is the other option, set them at the lowest and let the consumers, you know, set them higher if they want? I just don't think we can necessarily -- the consumer doesn't have that much knowledge at this point in time.

And as far as working with all the different players and stakeholders, I do notice, and I'll say it again, and I sound like a broken record, but the consumer groups are being left out of this conversation to some degree. And I really think we need to get them to the table. We're at the table with phone companies and banks, et cetera. We need to get to the table with the ISPs and the computer makers.

MS. YODAIKEN: Okay. Dave, you want to go ahead?

to really understand where they are at in their ability and their willingness to deal with some of these issues.

But there's no denial that the structure of our industry itself inhibits a lot of the solutions that we all think need to be implemented. I mean, we're talking about a very fragmented environment, on both the sending and receiving side. So, it's difficult to move -- be talking about more than just point solutions. And that's why I think having things like some of the things mentioned in the last panel are important.

MS. YODAIKEN: Okay, so we've got just a few minutes for -- we don't have -- I thought we bumped the time? No? Okay, apparently we don't have any time for questions.

Thank you all. Thank you, panelists, very much.

(Applause.)

MS. YODAIKEN: We're taking a quick break.

IDENTIFYING BEST PRACTICES FOR BUSINESSES

MR. TUMMINIO: Let there be light. Good afternoon. My name is Phillip Tumminio. I'm an attorney here at the Federal Trade Commission's Division of Marketing Practices. And on behalf of the FTC, let me welcome you to this segment of this year's Spam Summit entitled Best Practices for Businesses.

We've spent the better part of a day and a half discussing malicious, criminal spam. We've heard about bots, zombies, phishing, spoofing. Maybe it was even suggested that there's combinations, sort of a zombie-phishing-bot that spits from a server in Eastern Europe, something like that.

I like to think of this segment as sort of the silver lining to the cloud segment, the Yes, Virginia, There is a Santa Claus segment. And I say that because we're now going to focus on strategies and techniques that businessmen, marketers, entrepreneurs have developed that truly distinguish them from the malicious and criminal spammers whose only goal is to undermine e-commerce and to undermine the trust and functioning of the Internet as we know it today.

We're fortunate to have a panel with very deep experience in e-commerce, e-marketing and related consulting and advocacy, and I think you're going to hear

a suite of solution pieces that's going to include some technical fixes, in combination with some business practices and some ethical views, approaches to marketing, handling customers in general.

I'm going to introduce our panel, and then after that I will probably have a couple of follow-up questions, and we will take as many questions from the audience as we can and try to make up a little bit of the time that we lost earlier.

So, starting from my left onwards, Matt Blumberg, who is Founder, Chairman and CEO of Return Path, Incorporated. Return Path has assisted top marketers in building relationships, customers and generating higher response rates and returns on email program investments since 1999.

We have Mike Zaneis, Vice President of Public Policy at the Interactive Advertising Bureau. The IAB has among its objectives setting industry standards and guidelines for online and interactive campaigns and marketing. They represent over 300 companies engaged in interactive advertising.

John Mathew is Vice President of Operations at Epsilon. Since 1969, Epsilon has provided client-centric marketing solutions and end-to-end integrated services for e-commerce and marketing.

time, we sort of feel like, all right, well, we know all this stuff. We know about authentication at this point, you know, doesn't everyone else? And the reality is most businesses don't.

I had a room today of about 120 people, and I would say 115 of them didn't really know what authentication was. So, I think it's still fairly early days when we talk about rolling all of these best practices out to the world. But the good news is that there is an emerging consensus around what the best practices are.

So, legitimate mailers have every interest in helping to solve the spam problem. And very simply put, it's about the false positive rate for them around their email. Between one in five and one in four legitimate marketing emails, permission, the whole nine yards, don't get delivered to the inbox. And that's across a broad sample of ISPs and filters. Some, of course, are much better than others.

And what I always tell our clients who are multi-channel retailers is imagine printing 10 million catalogs and lighting two-and-a-half million of them on fire, because that's what happens to your email these days. And it's really enough to make a marketer absolutely mad. Marketers are still trying to figure

this out. We're still working our way down the pyramid or down the long trail, however you want to think about it. But the good news is that most of them do have a very keen interest in doing things the right way, once they know what the right way is.

And although there are lots of debates around definitions and semantics, there is, I think, a pretty clear line in the sand that's emerging on many of the mailing practices that separate the good guys from the bad guys. So, I think this panel is really going to focus on the different practices that mailers use to distinguish themselves.

And I think really the good news is that most marketers, direct marketers, email marketers, are quantitatively driven. They're used to managing metrics. And if nothing else has happened over the last few years in the industry, a lot of the practices around spam and around good email and bad email are starting to be quantified with common language to describe them, so they're becoming metrics that mailers can manage to. And everything around complaints, unknown users, all the reputation metrics that most of us in the room know about are things that are quantifiable, measurable and actionable.

So, I always say that areas of best practice

for mailers to focus on are very simple. It's how you get people on your list, how you get them on your list. It's about what you do with them on your -- when they're on your list, and it's about how you do that. So, get them on the right way, get them off the right way, treat them right when they're there, and do it the right way in terms of how technology supports your email program. And I'll talk about each of these for just a quick second.

So, in terms of how you capture email addresses and how you acquire permission and how you get people on your list in the first place, it's fairly straightforward. The good guys ask nicely. They're transparent about who they are. They set clear expectations up front about what kind of mail they're going to send.

The bad guys harvest addresses. They send without asking. They bury things in the fine print on their privacy policy and call that their form of consumer protection, or they do directory harvest attacks.

There is a pretty clear line between good and bad around permission. And if you want to think about things that are close to the line for a minute, it is okay to send email without explicit permission, right? That's what CAN-SPAM says in some circumstances. But I think most legitimate marketers get at this point that

there has to be a real legitimate business relationship and a reason to do that, because if nothing else, that kind of email will lend itself to more complaints, which will lend itself to worse treatment by the filters.

So, that's getting them off. Now let's talk about getting them off, how you unsubscribe people and manage your lists and how marketers need to learn how to say goodbye when people want to say goodbye. So, what do the good guys do? They actually don't just follow CAN-SPAM but they go beyond CAN-SPAM. They make unsubscribing easy; they make it work all the time; they make it fault-tolerant. They have a backup way of doing it; they honor it immediately; they work with third parties like affiliates to make sure that unsubscribe happens across platforms. And, fundamentally, the only people -- they only put people on the list that people think they sign up for.

Now, that's very different from the bad guys. They'll hide an unsubscribe behind a password. They'll make you go through all sorts of hoops and click many, many times over, do real heavy lifting. They'll ignore unsubscribe requests. Worse, they'll use an unsubscribe request as an opportunity to harvest an address, because they know they got a live one on the wire. Or, they may unsubscribe you from one list, but they'll just roll your

way than I'm hearing from you today.

Next, treat them right. How you manage the subscriber experience in between when they get on your list and when they get off your list. Show your customers the love. What do the good guys do? They're interested in things like relevance, targeting, sticking to their up-front expectations, segmenting, sending less mail in order to get better results, testing, monitoring, watching complaints.

And that's very different from the bad guys who send what they want, when they want, where targeting is not only irrelevant, but it's not even part of their lexicon. And I remember in the old days, my boss at my prior company used to say, you know, how many times am I going to receive spam for breast augmentation? It just doesn't make sense.

Finally, do it the right way. Make sure thatmake sense.

There are dozens of things we tell marketers around doing it the right way, from things like throttling the number of connections they have open to managing their bounces and complaint rates. But I'll focus on three big ones today to close up.

The first one, authenticate. Just do it. Many times in the industry we've compared this to just getting a driver's license. It's not going to stop spam, it's not going to prove that you're not a spammer, but it's a very, very important first layer in the war against spam. It lets ISPs and filters know who you are, and that's really the baseline of filtering, of how filtering works.

And I know there's been a lot of talk about authentication here already, so I won't spend too much time about this, other than to come back to the point that it is a long, slow, painful rollout of authentication across mailers and across that down -- as you move down the pyramid.

The studies that we've done out of our sender score reputation database indicate that probably only about 20 percent of IP addresses of legitimate mailers are authenticated today. And you probably hear different statistics if you talk to different people who measure this, but I can promise you, it is a fairly low number. And at the end of the day, authentication is free, it's

well as having images and links work, and, you know, it produces a lot of good advantages for mailers, provided it's priced properly.

The challenge with authentication is it's very hard to get, and that's because it is an E-ZPass into the inbox, and you don't just have to be a legitimate company to be accredited, you have to be in the top 5 to 10 percent of legitimate companies in terms of how you manage your email program from your infrastructure to your content to your complaint rates.

But back to the topic at hand, it's not just things like the whitelist that differentiate the good guys from the bad guys from the evil guys of the world. It's a whole bundle of behaviors, and I think the, you know, the things I've talked about cover a very small percentage of them. I'm sure the rest of the panel will fill in some of the other ones as well.

And I just come back to my speech earlier today at the Online Marketing Summit. It's not that those people don't want to be good, they just don't know how to be good. So, I think we all have a real important job in front of us, which isn't just about educating consumers, although that is important, it's really about educating legitimate businesses how to do things the right way and how to stay on top of that stuff as the rules of the road

change.

Thank you.

(Applause.)

MR. ZANEIS: Thank you very much. I'm afraid my presentation is going to pale in comparison a little bit to Matt's, but, Matt, consider your IAB dues paid for next year as an in kind if you help me prepare my next presentation.

So, I'm Mike Zaneis, I'm VP of Public Policy for the Interactive Advertising Bureau.

I run the Washington, DC, office here, and so I'd like to thank the FTC and specifically Phil for his efforts to pull this panel together, because this is exactly the type of reason that IAB opened a Washington office in January was to talk about all the good things that industry are actually doing, but then to translate them here to the legislative and regulatory field, as well. So, I think that this is an important event today, and we're happy to be here and to be a part of it.

So, IAB is really focused. It's a New York-based new media trade association, but we're really focused on all things in interactive advertising. And in

increase transparency across interactive sales and marketing activities. The document explains the most important terminology, the terms that we all use for email campaigns. And what we're trying to focus on is accountability and consistency across all the different actors.

So, just to give you an example, you know, coming up with a standard definition of a bounce rate or what a bounce is or what a hard bounce is versus soft bounce, because it really matters, if we don't have -- if we're not all talking the same language, if we're not all using the same metrics, then we're not on the same page,

So, and I think the important thing is understanding that the more tools we have out there are great, but if they're not being implemented and they're not being used by all segments, then they're not going to be very effective. And, so, we think education is the key to implementation. And, so, bringing together all the various segments, and I already talked about it, I think it's very imperative.

Talking about the best practices, putting them out there, so many of these are freely available and have had a number of the different segments engaged and involved in their development, so I think that's important.

And then something that people don't always talk about or associate with spam, and I think that's going beyond this spam problem and talking about things like, you know, how do we harden our servers and our websites, how are we protecting our Internet infrastructure? Because that's just as important as sort of fighting spam, because one leads to another. You know, you're talking about a delivery mechanism for phishing and the like.

So, I think every business has a duty, an obligation, to sort of look within itself and its practices and take some -- what are usually very simple

steps to do things like protecting your domain names or your company email and those servers, and keeping an eye out for phishing sites that maybe are exploiting your trademark, your brand name. Those are all very important.

And then I think what is sort of the point of this all is how do we sort of cooperate together, but then most importantly, how do we cooperate with law enforcement and how do we sort of help you help us, because in the end, that's what you're really trying to do here. You're trying to help us. You're trying to protect this medium, and you're trying to protect this goose that is laying the golden egg, and I think that that's the most important thing that we can do and then we take away from the summit is learning a little bit about what you all need.

And, so, it's been great to have some law enforcement on the panels, and to certainly be engaged with FTC. So thank you very much.

(Applause.)

MR. MATHEW: Good afternoon. John Mathew with Epsilon. First off, as I was looking around the room, I'm very encouraged by the number of people that are in this room. Back in 2003, when I attended this session, I couldn't even get a seat. I was actually standing back

there. So, I'm expecting that -- I'm hoping that the reason why there's this many people here today is because spam is less of a problem and concern for a lot of

So, first off, I have the requisite stats in terms of the number of message or amount of messages being filtered. I also have the requisite quote from Charles Stiles in this presentation. So, AOL filters as much as 85 percent of all emails coming in at the gateway. The effect for the consumers is noise.

So, in spite of all the messages being filtered, there are still quite a large number of messages that do make it to the inbox. A Consumer Reports stat that was shared earlier, one in two experienced high levels of spam. So, the -- so, one effect, one concept to keep in mind is the noise level.

The other concept is fear. So, with phishing, with the number of unique incidents in 2007 or as of 2007, 23,000 unique reports, most of them with hosting sites in the U.S., there is a continued fear in opening messages and the reliability of these messages, it being from who it says -- who they say it's being -- it's coming from. So, the end result of that is fear.

percent are using some sort of spam-filtering software; 73 percent know how to set the filter higher within their platform, and so they are taking more control of the messages they are receiving in their inbox. So, consumer control is another concept that describe the landscape.

One of -- the good news about the consumer control is they are -- they do feel that they're better protected against spam, so because of these -- because of these tools that are available, because of the education that's available to them, they're feeling like they can detect phishing incidents more and more now than they were able to several years ago.

They are aware of being infected by spyware, which was probably not the case several years ago. And slight decrease in terms of the number of spam messages

behind this blue or light blue box are some of the filtering that's used by ISPs, things such as content filters, whitelists, blacklists, user-level filters. And, so, when marketers are sending out messages, they have to be able to manage to get through each layer of filters in order to make it to the inbox.

But the level of information that's available is very limited. So, if you're looking at the other end of it, we receive a bounce code and, in some cases and from some ISPs, we get additional information through the use of feedback loops. But this is not the norm, at least the feedback loop isn't, and there is wider adoption today, but this is not necessarily a cause-and-effect situation. You can't always look at the end result and try to make their way back through and try to figure out what exactly happened.

And for a marketer, this is frustrating, so they are mailing -- they're sending their messages, they're trying to adhere to best practices, and one day delivery rate changes. And in an attempt to try to figure it out, again, there's possibly one data element, sometimes more than one, that they can use to figure out exactly what caused that problem. And, again, it's a high level of frustration because they can't figure out what it is that they need to do or what behavior they

need to change in order to be able to improve deliverability.

And, so, the technical aspect of it -- the technical challenge is another concept, and the fact that it's not necessarily consistent. Again, as I mentioned, they could be going through doing the same thing, sending the same type of content, and one day experience challenges.

Additional constraints within the specific channel, unlike other channels like -- or TV or radio, the characteristics of the receiver is very different. So, I apologize for the small text, but the point of this is that marketers have to worry about not only the target segmentation, who they're sending messages to, but looking at the domain level, what clients their consumers are using, how the message will be rendered, will the image be -- will it be off or on, will it make it into the bulk folder or not? So, by ISP there's different characteristics in terms of how that particular message gets rendered. And, you know, you don't have the same challenges in some of the other channels.

The other concept that I wanted you to keep in mind is the definition. So, yesterday we spent a lot of time talking about spam in the context of malware, in terms of spyware or things that generate spyware and what

Dave Lewis referred to probably as the evil types of messages. From the ISP's perspectives, that definition is a little different, and it's based on reputation. It's based on certain behavior.

So, some of the metrics that are used to determine whether a company's a spammer or not are complaint rates, possibly bounce rates or how many -- how -- what's the population of your list that are undeliverable, whether they're valid unsubscribe methods, hidden honeypot accounts, the extent to which you hit those accounts.

So, the definition has definiteep72.0000 531.m00 ng1.i00

about the potential value in those email messages. And other things such as data validation to make sure that they're not sending to bad addresses.

The next major stage is welcome, and it still surprises me today how many marketers are not taking advantage of this particular stage. It is the opportunity once they register to make sure that you send them a message saying, hey, by the way, you registered with us, you know, here we are, here's how you can recognize us and please add us to your address book so that you can continue to receive our messages.

Okay, where we've seen problems is clients not taking advantage of this and they wait three months, six months before they sent that first message. And by that time, consumers have forgotten that they've registered, that they've signed up. And of course they will hit the report-spam button, I don't remember signing up for this.

So, we encourage them to do that, as well as using the welcome stage as an opportunity to provide a unique offer that may not be available to otherrtunity to provide

And then a lot of techniques around the overall messaging in terms of frequency again, the concept of value, authentication, you've heard that. From an inbound perspective, bounce handling is critical from, you know, ISP's perspective from, you know, the technology perspective. But another concept is ESPs, and my fellow colleagues from other ESPs will attest to this, ESPs have good bounce-handling capabilities.

We provide records of undeliverable email addresses. A technique that we suggest is use that on their website, so if they know it's an undeliverable address -- now, the question is how many of them are asking that consumer when they log in to provide a valid email address next time they log in.

A preference page, best practice, so, you know, it was talked about earlier. You know, let it not be a binary option, make sure that clients or consumers have the option to be able to pick and choose which communication stream they want to continue to receive. And this is the stage you want to make sure your consumers don't get to. Once they get to it, you have no opportunity to get them back, so an opportunity to even provide a survey, say why are -- or why did you decide to leave at this point.

So, let me conclude at this point. If any of

you are interested in any of this information, as well as the research information we have, that's available on our website. I also recommend that you download MAAWG's Best Practice document that a lot of folks that are in this room helped put together. So, I encourage you to take advantage of that.

MR. TUMMINIO: Thank you. John?

(Applause.)

MR. INGOLD: My name is John Ingold. I represent BITS, and as Phillip mentioned, BITS is a membership organization. Our members are 100 of the largest financial services institutions in the United States. And I'm going to discuss collaboration this afternoon. We've already talked about collaboration a lot, in a lot of different ways. We've talked about collaboration between consumers and businesses, between private and public sector. We've talked about international collaboration.

But I'd like to focus on a different part of collaboration, one that might not immediately occur to you, and that's collaboration inside a specific industry. What I'd like to do is talk about what the financial services industry has done and is doing to address this problem as an industry. And then I'd also like to talk about how these lessons can be applied by other

industries that trade a lot of mail like our industry does.

We've talked a lot about the problems of spam, and I'd like to focus for just one moment on the specific problems that the financial services industry faces with spam. The first problem that we realize as recipients of mail is that we have an overwhelming percentage of our inbound mail is unwanted mail, just like everyone else. Our members rate approximately 90, even 95 percent of their inbound mail as unwanted mail. And, so, of course that is just an overwhelming burden, in some cases, on their email infrastructures.

But more importantly, as senders of mail, we need to be able to authenticate ourselves to our consumers, just like we have a responsibility as a regulated industry to know our customers when they come into our branch or when they are logging on online, we want our customers to know that when they get a communication from a financial services institution the communication is from the financial services institution.

And the other issue, of course, related to that is the issue of spoofing and phishing. A huge amount of the phishing and related bad acts that go on are aimed at financial services institutions. By some counts, seven of the top ten phished sites are financial services

institutions, and most of those are our members. So, this is an important issue to us, and it's an important issue for the industry.

To address these threats to our consumers and to our institutions, BITS and our members published a paper in April of this year called "The BITS Email Security Toolkit." This paper is publicly available on our website at BITSinfo.org, and we'd encourage you to look at it if you're interested in learning more about what we've recommended.

We have recommended three specific protocols to be adopted by our member institutions, also by our service providers and our business partners. TLS, which is Transport Layer Security, is one of these protocols, but it doesn't really affect the phishing or the spam issue that we're talking about here.

The other two protocols are Domain Keys Identified Mail, which Jim Fenton from Cisco covered very well earlier today, and either Sender ID Framework, which Craig Spiezle from Microsoft covered well earlier, or in the alternative, SPF, Sender Policy Framework. That's what we're recommending. And as Jim and as Craig mentioned earlier today, none of these protocols in and of themselves will solve the problem, but we are convinced that adopting these three protocols together

that we have chosen or the ones that you find necessary in your situation. We have a lot of technical expertise in our member institutions, but our members were not the ones that wrote the protocols. So, we have been helped immensely by the efforts of people like Craig Spiezle and Jim Fenton and Miles Libbey was involved in a meeting that we had, and Pat Peterson spoke yesterday. These and dozens of other people from the ISP community, from the email security community, from our business partners, our service providers have been immensely helpful in helping us shape these recommendations and in supporting our efforts toward implementation.

So, reach out to these folk, and even though none of them, I think, would probably support everything that we have -- that we are pushing for in our paper of the specific implementation methods that we are recommending, still in principle you'll find a lot of common ground, and I think you'll benefit from working with them as we have.

So, I would just encourage you again to work together with others in your industry towards that end.

(Applause.)

MR. CERASALE: Hi, I'm Jerry Cerasale of DMA, and I think the FTC for having me here. I see we're getting close to the witching hour, and I'm going to try

and go through quickly, because I don't think the FTC jurisdiction goes to stopping planes and trains in their schedules.

So, I'm a broken record: authenticate. You've heard before that DMA requires all of its members to authenticate their emails. The real key to this is if there's a greater percentage of authentication, we think there's a greater expectation of authentication with consumers and with ISPs. And that's the real key. That's the first thing we have to do. You have to get that platform before we go on further.

And if you remember what Margot said this morning, that she's afraid of blocking non-authenticated emails because there's legitimate email that would be lost there. So, we've got to try and take that fear away from the ISPs. That's a thing that we have to do.

We don't favor a plan from the DMA requirements, but we want to make sure that whatever authentication plans there are, they have to be compatible. We're talking about small marketers here. You have to think about the fact, the 80/20 rule that everybody talks about, you know, 20 percent of the marketers send 80 percent of the email, but there's 80 percent of the marketers that are still sending 20 percent email. They are very small companies. We have

to make it easy for them to authenticate, as well as teaching them to authenticate. So, it's got to be easy to use, inexpensive and only one, I don't have to go and sign up for four or five different authentication plans. That's really important.

One of the things we've found as we're trying to help our members authenticate is that our members have authenticated one domain from which they send emails, but they didn't authenticate the rest of them. And we're going through and trying to find that out. We're also offering a service to membership, a check, you know, kind of a report card of how well you're doing on CAN-SPAM, on authentication and so forth that our members, we hope, will start using. We announced that this week, so we hope they do it. And if you want to join DMA, please.

The other thing, once you send an email, don't forget about it. And this is really in part for smaller businesses. Examine the bounce-backs. Examine the opt-out rates. You know, whether it's an opt-in lister or not, the law says you have to have an opt-out on the email. Examine what the opt-out is. See your lists. Try and see where your stuff goes, whether it's getting through and what's happening to it.

If you're going to certain domains, certain IPs -- ISPs a lot, contact them. Find out what's going on.

Have a dialog with them. Because, remember, as Miles said, it's your reputation that's there with every email that goes out. So, try and remember that.

Partners. We really haven't -- I haven't heard a lot talked about partners here. Know with whom you are dealing if you're a member. It's got here -- is the list you have obtained current? I mean, is the list you're using current? If you're using a partner, let's go in with them. Is it a current list? Is the list a result of harvesting? Did they tell you it's an opt-in list? Is it really an opt-in list? What really is that?

What's the reputation of your partner? We've talked about your reputation being on the line, well, you have to do some homework to try and find out who -- what the reputation of the partner with whom you're using. That is really an important factor, I think, that you have to do to try and combat spam and try and make yourself different from the bad guys.

Address hygiene. It's one of those things that I'm back in my postal days. You know, if you send Jerry -- something to me, Gerry Cerasale with a G, through the U.S. mail, I'm going to receive it. If you put it with a G, Gerry Cerasale, on email, I'm not going to get it. It's not going to come to my email box. My last name is peculiar, it probably won't go into anybody's email box,

but whatever the case, it's very different as you look at email. You have to make sure your addresses are correct, and email correct change or churn much more rapidly than do postal or phone numbers. And the key here is to spend the money now. In all of this, spend it now before you send out the email so that it reduces the problems later.

Secure your servers. Don't become the foreign control so that it's going out there. That's important. We've talked about it. I don't have to talk about that any longer.

Honor consumer requests. Come on, these are your consumers. These are the people who you hope are going to buy from you. The last thing you want to do is ruin your reputation, have them angry at you. Make certain, you have an opt-out that's required, make certain it works. Check it. Check it today, check it tomorrow, check it the next day. Check it, check it, check it, check it.

Lois can smile here, because there was a case against someone, you know, the company spam filters blocked the opt-out requests coming back from their emails. You know, they were fined, a small one, because it was unintended, but make sure it works. Make sure your stuff works.

And you have 10 days to do it, come on, you can

try and do it faster than that. And that's not on the rule making, we need 10 days, but whatever the case, try and make it faster than that.

Now, finally, my last thing here, some crazy, off-the-wall stuff. You know, I'm the guy -- you know, I'm getting older now. When people talk about their mother or their father, they're starting to talk about me on these things, so I worry about it, but there are a couple -- two thoughts I really want to think about. We -- as you listen about filtering, it's usually at the destinating ISP. They have the filters up.

Well, the time to start looking and try thinking about filtering from the originating ISP, is it time to look at some resources and for our industry to start thinking about that, what that does is it stops some of that traffic from even going over the lines, as you block it earlier. Don't know how that can work exactly. I don't have an answer to this, but it's time to start thinking a little bit differently on filtering, I think.

Finally, on the consumer market, it was interesting to listen to the last panel. Most consumers, most consumers buy a computer and they want it to be a turnkey computer. I plug it in, I turn on, and it works, just like my car. I mean, have you ever been at a car

rental place when certain cars have different things, they don't know how to turn the lights on, embarrassed people come back, how do I turn the lights on in the car? They don't like that. They just want it to work.

Why can't we look at computers being sold to consumers being secure? Having ways to get them to be secure? We can do it. Let's start thinking about it from a manufacturer point of a view, from an operating system point of view. Let's get -- try and see some way to do that to try and combat the spam problem.

Those are just some -- and I don't have an answer. Maybe it's totally -- it can't work, but those are some thoughts, I think, to think about. Thank you, and I hope you get your planes and trains.

(Applause.)

MR. TUMMINIO: Thank you, Jerry.

MR. TEMPEST: Good afternoon, ladies and gentlemen. My name is Alastair Tempest. I'm a foreigner, because, as you've heard, throughout the last two days, this is really a global issue. It is very much a global issue. And I want to do -- just go a little bit, looking very closely at the time, away from the best practices to talk a little about Europe, because it has been discussed during the last few days as an area where spammers are now moving to. It's rather like squeezing

your toothpaste. You know, it ends at one end or the other end of the tube, and you've managed to squeeze the spammers out of the U.S., so they've come to Europe. Thank you very much, indeed.

But at the same time, many of you may have heard the phrase an Englishman's home is his castle. We are, as marketers and consumers, particularly in Europe, particularly sensitive to intrusion and to data privacy, or what we call data protection issues. There is a very

your toothpaste. You know, it ends at one end or the

We have enormous amount of legislation in Europe, at the European level, and that means at the national level, too, because the European level passes the legislation on. We have consumer protection laws on, for example, unfair commercial practices, unfair contract terms, et cetera, et cetera.

There are the criminal laws in each national country. And these things together, if you look at nearly any form of spam, could be used very effectively to stop spammers, because spammers break some rules or other, particularly the data protection ones.

The problem is the enforcement, and here I think we have a very big problem in Europe. There is an enormous confusion, even at the national level, between the different agencies who can take part in enforcing, between the data protection authorities, for example, or the communications authorities or agencies, like the Office of Communications in the U.K. There are -- the competition authorities. There are also, of course, the police and the consumer ombudsman. So, all of them fight amongst themselves, and the result is that you don't get very active prosecution of bad-doers.

Just also there are very subtle but extremely important differences between how the legislation pans out at the different European levels. Under French law,

Europe.

And, finally, we are also seeing sophistication of spamming, as you are here, hitting us very hard, indeed. We use SMS, small messages, text messages, mobile phones, et cetera, all this sort of thing is being affected by spamming. And spammers are becoming extremely sophisticated in the ways they're doing things.

And just another very quick example of that, which came out last month, a Swedish bank, the 200 largest investors in this small bank, were attacked by a spam, which asked for their PIN numbers, et cetera, et cetera. It was a Russian gang behind this, and they cleared over two million Swedish krona out of the bank before the bank realized and closed down the system six hours later. So, this is extremely sophisticated. It's using Swedish language, et cetera, et cetera. They knew exactly who they were after.

But what are we doing as an industry? Well, codes of practice exist. Many generic codes, specific codes covering email marketing within the European Union countries, within our own codes of practice at FEDMA, for example. The national direct marketing associations, the national IABs have email marketing councils who are working very closely also with ISPs.

Across Europe, however, the problem becomes much more difficult. And if you talk to the large emailers who do go across Europe, many of whom are, for example, travel -- online travel agents, like, for example, lastminute.com, they have to employ a whole regiment of people ringing the ISPs all the time to ask for permission to make sure that they're not being blocked, because within Europe as a whole, commercial ISPs are estimated at around about 10,000, and noncommercial, another 10,000.

So, we've been looking at the idea of white lists. I use the authenticity, it's incorrect of course, it's a difference between English English and American English. I mean very much whitelists. And I just brought two examples of that. One is the example in Germany, where the Certified Sending Alliance has been created between the ISPs, which there are over a thousand in Germany, and the bulk mailers. And that is together with the DDV, which is the direct marketing association.

2,dfsr7 i4000 in

will be a London Action Plan meeting in October here, but more meetings with the regulatory authorities and the enforcers in Europe and elsewhere to try and get people much more aware of what's going on.

Thank you very much.

(Applause.)

MR. TUMMINIO: Thank you, Alastair. We are very short on time. We have time for maybe one question. Are there any questions from the audience?

Not seeing any hands from -- yes.

AUDIENCE MEMBER: Maybe outside the jurisdiction (inaudible)... Maybe a bit outside the jurisdiction here, but as we've already got candidate stomping in Iowa and New Hampshire, do you think the concept of managing email outside the pure context of commercial is going to become a problem that we all have to start to wrestle with as political candidates and issue advocates start to engage and to some degree start to have to either do it the right way or many of them, I think, are doing it the wrong way and will have to do it the wrong way in order to get access to the inbox. What role do you see yourselves playing in helping to manage that process, recognizing it's not commercial, but it also still costs money?

MR. TUMMINIO: I offer this to the panel. Any

takers?

MR. BLUMBERG: It's a huge problem. There's no question that there's going to be -- there already is an enormous amount of political spam, particularly around campaigns, and that will -- that will just explode over the next year and a half. What to do about it? I'm not entirely sure. I mean, you know, there's enough gray area around the law, but certainly the systems that filter mail will have to take them into consideration. Reputation systems will obviously continue to measure and monitor those things. But it will be a big problem.

MR. TUMMINIO: I apologize, that is all we have time for in this session. Please don't wander off. We're going to start the next session in three minutes,

MR. SALSBURG: Could everyone take their seats, please? We're going to get started in about 30 seconds.

So, why was this conference called a summit? That's a question that a lot of us at the FTC have been asked. We could have just called it a conference, a workshop, a forum, a shmooze-fest, free trip to Washington for some people, a networking opportunity or just simply a meeting. Did we have a cool logo that we wanted to unveil? Did we like the alliteration, spam summit? Did we envision that this conference would end in some sort of grand arms control agreement? No, it was none of those.

When climbing a mountain, the summit is the place where you briefly stop to take a picture. It's the place that has unimpeded vistas. You can look back to see where you've come from; you can look forward to see where you're going.

So, these past two days, we've been enlightened by 47 panelists. We've learned about the increasingly criminal nature of spam, its use as a vector for malware and the creative and hard work that many in this room and elsewhere have applied in the fight against spam. From a very high vantage point, we've looked back. Now it's time to look forward and to plan the path ahead. And that's what the purpose of this panel is.

Obviously in this final session of the Spam Summit, we will not solve the spam problem -- or even really create a plan of action. But hopefully we can chart a course between now and about 5:15.

(Laughter.)

MR. SALSBURG: So, set your alarm and hold on, and we're going to try to have a very fast ride in developing such a plan. And helping me do this are some very incredible panelists. First, to my left, is Tom Grasso. You've heard from him already here, so many of you know who he is, but anybody who just happened to drop in, he is the Supervisory Special Agent with the FBI, and he has developed the National Cyber-Forensic and Training Alliance, which is a joint partnership of law enforcement, academia and industry.

Miles Libbey, Senior Product Manager at Yahoo!. Miles is one of the coauthors of DKIM, the authentication standard. Miles informed me that he will be heading to Yahoo! Sports as of Monday. This is his swan song. Perhaps he will be able to authenticate Barry Bonds' blood tests.

(Laughter.)

MR. SALSBURG: Brendon Lynch is the Director of Privacy Strategy and Microsoft's Trustworthy Computing Group and a member of the certification board for the

International Association of Privacy Professionals.

Michael O'Reirdan is a Distinguished Engineer at Comcast and the Vice Chairman of the Messaging Anti-Abuse Working Group, or MAAWG. I hope someday that I could have the word distinguished in my title.

MR. O'REIRDAN: You haven't got enough gray hair.

MR. SALSBURG: Phyllis Schneck is the Vice President of Research Integration at Secure Computing Corp., and she's also Chairman of the Board of Directors of the InfraGard National Members Alliance. InfraGard is an FBI-sponsored public/private partnership comprised of thousands of members of the public who are dedicated to protecting the nation's infrastructure.

And, lastly, Charles Stiles, he is AOL's

should be doing as we chart a plan of action.

But, first, let's consider, are there other entities we haven't thought of. And, so let me throw that question out to the panel. Who do we not usually reach out to that really has a role to play here, now that the spam problem, we've learned, is more than just about spam, it's about threats to the infrastructure of the Internet.

MR. O'REIRDAN: I wouldn't mind taking that. I mean, I think one of the areas that we can look out to is the intelligence community. I mean, they do an awful lot of analysis of traffic. They're continually analyzing traffic flows from, you know, data going from A to B. And I just wonder if they've got any interesting technologies that may be -- you know, sometimes things can leak out. I've seen that once or twice, and I think it might be an interesting area for us to look.

MR. SALSBURG: So, some sort of meeting with -- secret meeting with the NSA might be the --

MR. O'REIRDAN: Well, I'm a foreigner. I'm probably not allowed to have one.

MR. SALSBURG: Are there any other industries that need to be consulted that might have something they can help out with here? Miles?

MR. LIBBEY: So, over the last couple of years

in the anti-spam world, we've had the beginnings of the academics beginning to get involved. So, there's a couple of conferences now, CAS is an annual conference, usually held in the Silicon Valley. There's a -- kind of a quasi-academic conference at MIT that usually talks about Bayesian philosophies and I don't usually see the academics typically represented here.

MR. SALSBURG: How about middle-school students? I mean, are we missing out on this generation of really smart, technologically savvy people that might have some insights into new scams?

Any better ideas?

MR. O'REIRDAN: Well, if I had seen in the U.K., I've seen high school students reached out to to help design satellites, so I'm sure we could have a good go at trying to get them to do anti-spam stuff. I mean, a competition always attracts people.

MR. SALSBURG: Are there industries that are affected by -- that are more affected by malicious spam than others that might have a vested interest in spending some of their money on the fight?

MS. SCHNECK: We heard a lot today earlier, it was touched on several times about danger from spam, other than the ad for the drugs showing up in your inbox. I heard a great phrase earlier, the E-ZPass to the inbox.

Consider for a moment the E-ZPass to the Internet. I mean, these guys are sending whatever they want, it's arriving on your network whenever they want. So, look at that as an infrastructure protection threat, and there you have, according to Presidential directive HSPD 7, you have all 17 critical infrastructures, you know, Energy, Transportation, Emergency Services, everything that runs the systems to keep that light on, and then consider the fact that the bad guy has the ability to send whatever he or she wants to that network.

So, we need to look at the infrastructure protection community, working with Tom Grasso, working with the ISPs, working with law enforcement, and really focus on, I think, three things. You know, one is just that coupling of the expertise in the private sector with law enforcement and everybody getting along. I know that's a well used phrase, but making that happen the way Tom's group does.

And the second is looking at the vulnerabilities. What does it mean? You know, spam has migrated from the middle school kids and the hackers that think it's cool to get a virus all the way into organized crime making money. And now it's cyber warfare. That's the reality. So, looking at what those vulnerabilities are.

And, thirdly, as a country, working on that security versus convenience juggling act that was brought up earlier by the gentleman, I think, from StrongMail. And forgive me if I've forgotten your name, but that's a great analogy and you're balancing that constantly. So, things like the FTC working together with industry to show you how to balance that out while at the same time you're protecting your infrastructure.

MR. SALSBURG: So, if what we're talking about here really is a risk of cyber warfare, then perhaps Michael O'Reirdan's point that we need to reach out to the military is a sensible one.

Charles, do you have something to add?

MR. STILES: I'd just like to see Tom kick in some doors. I think that would be an exciting thing for us to see. Certainly we need more criminal enforcement, and I know that sometimes the resources are not always there. But there's an awful lot of collaboration that's going on within this industry and also outside of this industry, with the educational institutions, with the financial industry, with law enforcement, with legislators, both domestically and internationally. But I think when we start to see more criminals go to jail, that's going to be the biggest deterrent.

MR. GRASSO: Yeah, and, you know, I'm

if they so choose to activate that feature.

Are consumers really doing enough? Is having things like free anti-virus software enough and security patches enough? Or should we -- or should ISPs just simply refuse to provide connectivity to consumers that don't have this stuff?

MR. STILES: I think that relying solely on the consumers for this is certainly the wrong way to go and putting too much reliance upon consumers is not the right way to go either, because you have to have some consistency there. I think that, quite frankly, ISPs and solution providers own the burden there, and we need to make sure that we're doing what we can to stop this stuff before it reaches the consumer.

MR. LYNCH: And what I was going to add is you mentioned a number of technologies that we do provide for consumers to protect themselves, but the key challenge is for them to be able to use those in a way that really does protect themselves. And, so, this probably will overlap with -- as you might have with the technology industry, but I think we all have it upon ourselves to make it very simple. And whether it's default settings, whether it is simply consistent consumers to be able to make trust decision.

Today we offer them so many different symbols

an absolute minimum reimaging or something that we can do that's going to allow those PCs to be clean when they get to the network?

MR. SALSBURG: When I buy -- again, I buy a new PC, and I bring it home and I plug it in, and I plug it into the Internet. The very first thing that happens, I assume, and correct me if I'm wrong, is that my operating system checks to make sure -- goes off to a server somewhere and there's a check to determine whether or not I have a genuine copy of the program, of the operating system.

MR. O'REIRDAN: Because what happens is actually the -- what happens in a lot of cases is the user interrupts that search that's going off to the update site, and it says, oh, I want to see the latest football or something, so in the next half-hour they've been surfing back and forth on the net and they've been exploited.

MR. GRASSO: Yeah, I mean, this might -- it might be beyond the scope of this discussion here, but I think the problem or part of the problem is that computers are incredibly complex devices, probably more so than they need to be for the average person that's using them. And I think this is, you know, where we get into all of these issues, when you think about all the

different things that you can do with a PC, all the different functionality capabilities that it has. I think it's akin to if you went to a Lowe's or something like that and were able to purchase a 747 and give you the keys and say drive it home. Well, I mean, when you think about it, what -- when you think about the level of expertise you need to fly a 747, what sort of expertise do you need to really understand what's going on in that computer and how many people have that expertise that are using them? So, I think that's -- I don't know if we want to get into this or not. I mean, I really think that's part of the problem is that these are incredibly complex devices that we're delivering into the hands of people that are not engineers.

MR. SALSBURG: But I guess that's the point, Tom, is that we have these incredibly complex machines and our advice is fairly complex, also, isn't it? It's make sure you have a properly configured firewall. And is there other advice we can give consumers that's just more basic, that might help? Such as unplug your Internet connection when you're not using -- when you're not on the computer. Unplug your computer and turn it off.

MR. GRASSO: I think there is advice, but as with Brendon -- excuse me -- as Brendon was saying, I

think we have to make is simple. I don't think we can rely on the users to make the correct decisions. You even look at the complexity or how good phishing sites are these days. Even if you know a lot about computer security, it's really difficult to look at a phishing site and know whether or not it's the real thing, okay? These guys are getting good as far as spoofing the URL, even making it look like the padlock is there and that you're really at a secure site. So, okay, so I guess you can check the fingerprint on the certificate, you know? I mean, but, I mean, these are all things that I think are beyond the average consumer. I think we need to make it simple for them. It has to be easy for them to implement these solutions.

MR. STILES: You also need to consider the convenience factor. So many of the features that are built into programs today call upon the convenience to be able to log in and use your computer when you're away from it, to turn on the camera so that you can see inside your home, to print things off, to retrieve documents. This is all convenience that is gone once you start securing it significantly. Even websites that you might want to visit that get blocked. It all plays into convenience.

MR. SALSBURG: So, then, advice to just turn

off your computer may be bad advice for a number of consumers?

MR. STILES: Correct. And you may not be getting the updates that you really need to receive.

MR. LYNCH: And, also, when you look at vectors like phishing scams, you know, they're obviously when the computer's on. And I think the PC has its challenges, and there are a lot of things that we can do, companies like Microsoft, as operating system providers, too, for

fundamental issues, I think, with the Internet that really need to be addressed, as well. And if we could solve that, the incentive for the bad guy to use spam as a vehicle for phishing would go away. And I'm talking about things like stronger mutual authentication, to be able to enable the individual to authenticate the website that they're going to. We make that very difficult today. It's a key area for industry to focus on. Extended validation certificates in the browser are a step in the right direction.

But one of the other core problems is that we're sharing secrets online. We're being asked by banks and retailers and others to provide usernames and passwords and the real root cause of the identify theft and online fraud problem is that the bad guys are able to intercept those credentials and reuse them for the fraud.

So, if we can focus on actually changing the game, and you could see a future where things like online fraud and identify theft would go away, if we could find ways to simply put things like public key cryptography in the hands of users without them knowing it, where secure tokens are being exchanged for online authentication rather than them having to enter passwords and PINs and usernames.

MR. SALSBURG: So, then, I think what you're

suggesting is that a comprehensive solution to the spam problem is really a comprehensive solution to a lot of problems and that we need to think pretty globally here.

MR. LYNCH: I think you're right. And I was particularly focusing on online fraud and identity theft, which causes a lot of the fear and the erosion in trusted confidence. Maybe it's different when you look at a pump-and-dump scheme. It's a different problem to solve, and it requires different solutions. But certainly there's probably some commonality among a number of them.

MR. SALSBURG: Well, let's move on to what ISPs can do. You know, the ISPs are the gateway to the Internet and in a very strong position to help reduce the problem of malicious spam. Two weeks ago, for those of you that follow the FTC website and our consumer advisories, we issued an advisory about an email that was supposedly sent by the FTC. The email claimed to acknowledge that a complaint had been filed by the recipient, and it included an attachment.

Consumers who opened the attachment to this email unleashed malicious spyware onto their computer. In case you're wondering, this email was not really sent by the FTC. The FTC publishes SPF records, and so these SPF records indicate that the IP addresses of the servers it sends email from, and the bogus email obviously was

not sent from these IP addresses.

So, Brendon Lynch, Microsoft is the driving force behind Sender ID for email. Is it correct that these emails would have failed the Sender ID test?

MR. LYNCH: I must admit, I'm not exactly close to the details of, you know, how that would work, but I think what this points to is the bigger question that authentication alone is not the -- not a silver bullet solution. And there's been a lot of talk over the past couple of days about the need for authentication plus reputation. And I think a proper combination of those two would really have helped in this regard, because the reputation side of things would have said, you know, this is not the FTC, this is something new.

MR. SALSBURG: Well, I would imagine that when an ISP, if it's filtering based on it or doing any sort of analysis based on Sender ID or SPF records, is going to see either a match between the sending domain's IP address and the IP address in the -- between the IP address that appears in the email and the IP address that's in the SPF record. Or, there's going to be no match; or there will be no SPF record; or the SPF record will be improperly configured.

If there is absolutely no match, so there's an SPF record there and there's no match, why would an ISP

still deliver the message?

MS. SCHNECK: I would agree that this is about not only authentication, who you are and proving who you are, but also what we've seen about you, because no match could -- no, I'm sure the FTC does everything right, just preface it with that, and I'm the last thing between you and happy hour, so I'll try to keep everybody awake, but there could be a lot of reasons why there's no match, somebody just didn't publish at all, somebody brought up a new legitimate domain. So, it's a big key component of an even bigger required solution.

Another piece of that is reputation. So, obviously the IP addresses that were sending out the

behavior is, how much email volume he sends, what bad URLs he's affiliated with, how many times he's sent malware.

And, generally, these guys have a bad reputation, so even if there was no match but we knew they were bad, then it would have been blocked based on one of those. And there are hundreds of other tests that you can do that -- or us and different industries within the greater community are using.

Think about airport security. If somebody knew you were a good guy and you didn't have to put all your shampoo in a baggy, would that make life easier? That's the reputation technology versus the content. But when we don't know enough about who you are, then they start looking at your shoes and the hair barrettes and whatever, because they have to make sure any way they can.

MR. GRASSO: Yeah, I agree with what Phyllis is saying. I can say I've seen enough of these scams that even if there was a foolproof way to determine if something from FTC is really from ftc.gov that these guys are just sending out from ftc-security.com or something like that, okay? So, it would come from some domain name that isn't even really FTC and people would still see it and not know any difference and open it and respond to

it. So, yeah, I think you need more than just the -- just the proving where it comes from aspect to it.

MR. SALSBURG: Let's say that -- well, I would think that different organizations have -- they appraise the import of their reputation differently. And, so, for an organization like the FTC, who are much more concerned that an email that claims to be from the FTC really is from the FTC, then we are about a false-positive, about the fact that some communication will end up being filtered out.

A bank may take the same position; a marketing firm may not. Is there any way for an organization that sends email to identify to ISPs how they want to have these hard failures treated?

MR. O'REIRDAN: There's some work going on in the IETF, which is the send-assigning policy stuff, which is going to allow us to develop policies for the -- you know, for how you want -- for a sender to say how they want their mail to be handled based on their signature. And that's still in the IETF and being worked on at the moment.

MR. SALSBURG: Miles?

MR. LIBBEY: It's kind of curious. I mean, if you're going to send a mail, don't you want it delivered? I mean, it seems like you should -- if you're going to go

to that effort to create this thing and you should actually have a desire and -- to -- that consumers are going to want to read this, otherwise, don't send it, right?

So, there's always -- in all these conversations, there's always a tradeoff, and any kind of security you have, you know, whether it be, you know, the risk of a false positive or extra time or expense or complexity or what have you, you know, and so this is yet another tradeoff that you could make. It's just kind of a bizarre one.

MR. SALSBURG: But what is the benefit to a business to spend all this money to redo its way of sending email, publishing SPF records or figuring out how to use DKIM if there's going to be no big bang at the end when their domain is abused?

MR. LYNCH: What I was just going to say is I think Craig Spiezle down the back there wants to make a comment, which would probably address your SPF question more directly.

MR. SALSBURG: Sure. Craig?

MR. SPIEZLE: Craig Spiezle from Microsoft. So, specific to your case, unfortunately the FTC configured their record with a tilda-all, and what that means is that it does not have a receiver network to make

a definitive decision. It really says, these are my IP addresses, but there may be others. So, as a result of that, the way you configured it wasn't wrong, but it was not conclusive and it did not give the receiver network enough direction on how to handle it. And, so, by default, the way you designed it is the way it was handled, it went over receiver networks that would have checked but would not have deleted it. It would have maybe junked it, or may have put a warning on it. So, that's an example of where I mentioned earlier that organizations need to move to dash-all records, provide receiver networks that give definitive direction on how to handle a record that fails or is spoofed.

MR. LIBBEY: Just to add to that, there's -- so it's also possible that the bad guys didn't spoof the mail from the bounce address, which is what the SPF authenticates. So, it's possible that it would have passed that way. And at Yahoo! we find hundreds, if not thousands, of new forwarding servers every week.

So, there is risk, when you're sending to consumers that you're going to send to universities and whatnot or other companies or ISPs that end up forwarding to other folks. So -- and those do fail path based authentication techniques. So, there's -- you know, there are a number of ways that things could fail in this

case.

MR. SALSBURG: We heard from Des Cahill at Habeas that 13 percent of SPF records were misconfigured. Does this indicate that we need to do more to educate businesses who are setting up their SPF records on how to do this? Obviously we need to educate the FTC t's for the

MR. LYNCH: I think the obvious answer is yes. I think these were not necessarily syntax errors, as he mentioned, they were more incomplete records. And I think the number is a bit smaller, but I think clearly with any tool that can be used here, whether it's for the consumer or for the -- for any or,ht0izaione as proerc1.00000 0.00

until ISPs actually can start acting on authentication there's no real incentive for businesses to make this effort?

MR. STILES: I think that ISPs will start to gather additional information and start to work with reputation systems, as well as vendors and solution providers will start to build those reputation systems even more extensively than what we have today. And as these reputation systems start to build, then there is an absolute benefit, not only to the receiving networks that can make determinations as to whether or not they want to receive that message, but also to the mailers who can rely on the positive reputation to make sure that their mails are, in fact, being delivered and that they don't have to deal with the noise from all the junk that might otherwise be delivered.

MR. O'REIRDAN: Yes, I mean, for example, as far as in the third quarter of this year, Comcast plans to deploy a new system, a new mail system called SmartZone. And inherent in that will be DKIM and SPF. We're going to be checking inbound DKIM. One of the things we're looking at doing is going off to the people who send us the highest volume of DKIM-based traffic and saying in the absence of SSP, what do you want us to do with that traffic. For example, I believe eBay, and I'm

not putting words in their mouth, but I believe eBay has said, if it's not signed by us, dump it.

And, you know, I'm going to go off and talk to eBay and say, is that actually what you mean? Is that what you mean if PayPal -- you know, and then we will implement those policies based on what they want us to do, but only for a limited subset of traffic.

MR. SALSBURG: And is that kind of program limited to Comcast? Or if the FTC were to have a differently configured SPF record and want to say don't deliver messages, are there other ISPs we could go to and say the same thing?

MR. O'REIRDAN: It kind of works -- I mean, the problem is that there's no automated systems around at the moment, and that's what SSB is intended to be. And we can only handle so much in the way of manual systems, so that probably -- it would be -- it would be for large -- it would have to be for very large senders.

MR. LIBBY: So, at Yahoo! we have started doing it on a case-by-case basis, some rejections of both forgery mails and mails that have no signature for specific domains. And I also think you'll see -- going forward, we'll start to see some tools from ISPs that will help. I know on the authentication panel, both Jim

and Craig talked about it was a really -- business had a really tough time going off and finding -- or figuring out their infrastructure. I think you'll see more and more tools from the big ISPs saying here are all the IP addresses that we're seeing your mail from. And, so, you know, maybe that's a good punch list to go look at and see if you do have that third party that you forgot about or, you know, what forwarding IPs are sending your mail and what have you.

MR. SALSBURG: So, I take it that none of you would be advocates of some sort of date certain by which all email must be authenticated or it won't get delivered? We're just too far away? No publish or perish date?

MR. LYNCH: Deafening silence.

MR. SALSBURG: Okay.

MR. STILES: It is too far away. I mean, when everybody is publishing an authentication mechanism of some type and most receiving networks are checking that, we still have to rely upon reputation systems. And by not having some type of authentication in place, do we know that it's bad? We don't necessarily know it's good at that point. There are a lot of determinations that still need to be made.

MR. SALSBURG: Phyllis?

MS. SCHNECK: That's also a really tough decision to know when you can say, okay, we're not going to deliver a certain message as an email security provider. The worse thing ever is the email that somebody wanted that didn't get delivered and that always went to the CEO of the company. That's just how it works. And you never want to be the guy that blocked it.

So, as an industry, we have to come together, but that's a tough, tough thing to do to put the line in the sand and say when are we going to stop delivering mail.

MR. SALSBURG: Miles DKIM, was just approved by IETF as a standard, and it was approved in May. To an engineer, the 60-page standard may be a light read. To me, it was fairly impenetrable.

And the question I have for you is how realistic is it that somebody like me, somebody who's not technologically sophisticated, is going to be able to create a public/private key pair, figure out how to publish the public key and engage in the cryptographic signing of messages? Is this something we can realistically expect?

MR. LIBBEY: So, as -- I don't expect that you're going to be doing anything with your outbound mail. I expect that your IT department is going to be

dealing with the mail that you -- you know, you're going to primarily send mail from some web -- or some client, either -- maybe it's Web Pace, maybe it's a desktop client, and so when you click the send button, it's going to go to your IT department's submit server, and that submit server is going to authenticate. And, so, for the IT department, no, this is not that difficult. This will be an installed software. There's -- almost every vendor that spoke at this conference has some product out there that has DKIM imbedded in it or will very, very soon. So, I'm -- it's -- this is not that complicated.

MR. SALSBURG: So, I can set up an SPF record probably incorrectly by using a wizard on the Microsoft website. Is there any similar sort of wizard on a Yahoo! website that would do this for me?

MR. LIBBEY: Well, so, what you do is -- yes, is register for a yahoo.com account and then the message will be signed.

MR. SALSBURG: So, I was out having a cookie out at the table earlier, and I saw this very nice flyer on DKIM. And it tells me that there are three easy steps to do to participate in DKIM if I'm a sender. One is to compile a list of incoming and outgoing mail systems. So, I'm imagining myself as a small business that might operate my own server, so I don't have a complex number

of different domains. So, that's probably an easy one.

Determine who is legitimately sending messages using my name. Well, assuming that I don't out source anything, that's an easy one, too. And the third one is identifying implementation partner. What is that?

MR. LIBBEY: So, it's just your -- whoever -- whatever submit server that you're using or would like to use, you just upgrade your software.

MR. O'REIRDAN: Whoever makes your mail platform.

MR. SALSBURG: Okay, so I'd have to pay for some sort of upgrade?

MR. LIBBEY: A lot of these -- I mean, there are a lot of services out there that are free and an open source. So, they're --

MR. SALSBURG: I'd have to pay somebody to figure it out, though?

MR. LIBBEY: If you don't have an IT -- if you don't have an IT department that you're likely already outsourcing your mail.

MR. SALSBURG: Okay. Would it speed the wide-scale adoption of DKIM if there was some sort of free service to provide small businesses with --

MR. LIBBEY: Say like Yahoo! mail?

(Laughter.)

National Guard, some areas of the military. And basically it's a good private sector resource for the government to reach out and kind of find the transportation person that knows something about banking and vice versa.

What we are trying to do more of with this membership, and I was actually talking to John earlier about this, is tap them more for their knowledge and say what are things we can get and understand and learn from this group of people that we can bring back to government or to other companies and help us all sort of better prepare ourselves, better protect our infrastructures, because, quite frankly, the bad guys work together very well.

And one thing -- one set of statistics that we have from last year's, there were about a hundred new FBI cases opened that go back to information from the InfraGard membership, and the InfraGard membership assisted in about 101, or pretty close to that, cases. And that's separate from the other hundred. And we're guessing that that's probably only on about a 25 percent reporting rate, because no one tells government anything.

So, one of the new sets of stats is almost double that, that I just saw yesterday, for this year, and that's on about the same reporting rate. But, so,

the security of the DNS system, which is it secure enough? Are both these based on, you know, a foundation of clay? Anybody not want to take that?

MR. O'REIRDAN: I'll just sit here watching, you know, how long DNSSEC and the endless arguments that go on about DNSSEC. To be honest with you, I don't participate in them, keeping up a running DNS system that works really well is very important for a major ISP.

the A record of Amazon.com or eBay or PayPal, so if we're going to use it so that a consumer's going to go to a website and use -- do financial transactions over it, then it's secure enough to handle an authentication record.

MR. LYNCH: And what I'd add is I think your last two questions have really once again highlighted the need for reputation as well as authentication. And, you know, that's the way we've been doing that for some time, to have both. Alone, it won't solve it.

MR. SALSBURG: Do ISPs generally share information well?

MR. STILES: Yes, they do. Remarkably well. MAAWG is largely a collaborative organization, not just with ISPs sharing information with one another but also with vendors, mailers, solution providers and even the academic community, as well. I think information is actually being shared very well.

MR. SALSBURG: Is it based on the same model as anti-virus companies, which share definitions, they share their research and they compete on marketing?

MR. STILES: I think that all the barriers to competition actually fall once we enter a MAAWG organization. It is very much a collaborative effort. Our goals are the same. We're not competing as different

And through InfraGard, through projects like National Cyber-Forensic and Training Alliance, we're trying to make that real and make that happen, so that it's just not something that, you know, we say, oh, yeah, it's a good idea, we need to do it. I mean, through those initiatives, we're trying to make it something that happens and happens on a daily basis and turns into good cases.

And it is happening. All of the major cases that we've had relative to spam over the last couple of years since we started fighting this fight, it has all come out of cooperation, initiatives, that our cooperation between private sector and government. That is what's making this stuff happen, and that's what's making it successful.

MR. SALSBURG: Now, each ISP, I imagine, has its own set of honeypots when it's looking for spam and for other malware that may be in the spam. Do you share honeypot information?

MR. O'REIRDAN: Not currently, but --

MR. SALSBURG: Should you?

MR. O'REIRDAN: -- I believe that's an area that we should be looking into, just as I also believe that I'd like to see the vendors of anti-spam devices working on some sort of protocol that allowed us to share

realtime attack data, so that if I got a -- you know, if a company running Onport was attacked and I'm going to be running Bazanga, the Onport device could pass to the Bazanga device. You know, I'm getting realtime -- I'm getting attacked in realtime. You want to watch out for this, because, quite often, you know, an attack will start on one company, then it will come to another. It might be slightly varied, but it will be probably coming from the same set of IPs. They might just change a little bit by little bit. And I think the ability to share realtime attack data would be very important.

MR. SALSBURG: Is that something that MAAWG is working on?

MR. STILES: It is not, but one of the things you need to consider is that the attacks at different ISPs may be varied significantly. I may have a set of honeypots that gets a stream of traffic from a particular IP address or from a particular network. It doesn't necessarily mean that that same IP address or network is going to attack any other ISP or mailbox provider.

MR. O'REIRDAN: Yeah, I think some of it also tends to vary between the industries you work in. I mean, you know, cable we do find quite often that things will be relatively similar between -- you know, the attacks will be relatively similar across -- into the

same cable companies.

MR. SALSBURG: If you don't compare the data from the honeypots, how do you know whether or not they're similar or dissimilar?

MR. O'REIRDAN: Well, we know -- we talk to people -- you know, as you say, people do talk to each other. You know, we cable companies talk to each other and we've been -- you know, we do share, you know, that kind of level of information.

MR. STILES: And speaking on behalf of AOL for this particular statement, I can tell you that some of the attacks we've seen are geared specifically to AOL customers. And I would suspect that that's the case at other providers as well.

MR. SALSBURG: Margot from AOL earlier talked about how AOL had a really good fix on the fast flux problem. I think that's what it was called, fast flux? Yes. Is this the similar experience of the other ISPs around the panel?

MR. O'REIRDAN: We've got techniques that we use, but we can't -- you know, there's a point at which I don't believe we do share that.

MR. SALSBURG: Even among ISPs?

MR. O'REIRDAN: What's the American for no comment?

doing enough? Or are you all having a difficult time still differentiating their email from the spam?

MR. STILES: I think that legitimate marketers are actually doing exactly what they need to do. There are some exceptions to that rule, of course. MAAWG recently released the best practices document for mailers, and we don't see that as being a document that mailers need to follow as a step-by-step guide in implementing all of those steps, because certainly if you're having problems with delivery, those are things that you should look at and consider as possible aids in being able to deal with it.

But largely the legitimate marketers are doing exactly what they need to do. They're being forthright with what they're sending; they're looking at the data that they've got; and making the right decisions about what they send, to whom they send and how they send it.

MR. SALSBURG: Is there anything else that they could be doing that would enable you to ratchet up the filtering on the illegitimate marketers?

MR. STILES: Right now, no, I don't think so.

attribute reputations to those mailers much better. But right now, I think they're actually doing what they need to be doing.

MR. SALSBURG: Phyllis?

MS. SCHNECK: I think legitimate marketing is a great example of where looking at the content by standard methods doesn't tell you what you need to know, that versus the spam, because it could be a legitimate drug or it could be a legitimate mortgage ad that you actually wanted to receive. And that's where it's so important that we get, as a community, the authentication straight, the reputation straight.

And the reputation system, the bigger it is, the better. It's seen more data. You wouldn't go to a doctor that -- on his first day, would you? You want something that's seen the whole world's worth of data. So, one ISP, that's where we as a community have to start sharing more information, one provider, another provider, ISPs, so it's not just based on one person's or one ISP's reputation system. The bigger on those, the better. And direct marketing is a great example of why you need to know who it's coming from.

MR. SALSBURG: Do the reputation services, the private companies, a number of them participated here today, do they share information, or are they -- they

make their reputation scores and if you happen to purchase their product as an ISP, you use their product?

MS. SCHNECK: I think typically -- the financial sector does this stuff very well, and one example that's been told to me is they all walk on Wall Street and they're all there. The head of one bank is there, and he talks to Charlie, the head of another bank. And they share information this way. We're people, that's how we communicate. So, even if an industry doesn't have formal methods in place yet to share this type of information, and some of us do, some of us share a lot of information with a lot of different groups. I think that people communicate this for the greater goods at a lot of times that isn't generally seen.

MR. STILES: I think that right now a lot of the reputation systems that are in existence, because they want more information, are willing to share that with ISPs pretty freely. I know a number of them are offering that for free. But I think that we need to look at this as not a reputation service that provides a yes/no as to whether we deliver the message or not, but essentially like a credit score, depending upon the level of load or the amount of email that's trying to be delivered or the type of email that's being delivered, I might query one, two or three reputation services.

Now, if they were all sharing the same information with one another, I would just get one analogous answer, and that's probably not what I want, because I think for different messages and different mailers, we're probably going to be looking at different levels of reputation and different accuracy levels for each of those providers.

So, I think that we'll look at something like a credit bureau at some point. Some bureaus provide better information on certain types of loans than others.

MR. O'REIRDAN: I mean, there is also the case where you may want to tune your reputation services. I know there's someone working out, and I think it's called Comosphere, they're working outre workmdpr, and that's probably no

some people -- a lot of people would say yes, and a lot of people would say no. And, you know, that's not one answer. So, you know, our Taiwanese users might have a different answer for the folks that use our service in Russia, which might have a different answer for the -- than the people that our use our service in the United States. So, it's a -- reputation is interesting in a particular context, in a particular community. It's -- I think it can be quite distinct.

MR. LYNCH: Yeah, what I'd say to build on that is that good marketing practices will be driven increasingly by consumers as we give them the controls to vote on what they define as spam and what that means to them. And the differences are not necessarily just cultural, it's also within societies where there's a -- the tolerance levels are different. And, so, increasingly those feedback loops directly from the consumers will provide the marketers with even more data on how best to tune their practices.

MR. SALSBURG: If we were going to end right now, which we're going to pretty soon, and draw up the plan, what would be the one thing each of you would want to have in it?

Tom, why don't we start with you and work our way down to Charles?

companies and in other companies, who are working to fight this battle. So, to those of you who are dedicating your career to this fight, we at the FTC thank you and applaud you.

(Applause.)

MR. SALSBURG: Conferences and especially summits don't occur without the tremendous inspiration, coordination and perspiration of a large number of people. So, let's please give a round of applause to the following FTC employees who have made this 2007 Spam Summit such a success.

First of all, our dedicated tech staff for going above and beyond in terms of making sure that we have everything we need. There wasn't a single glitch in this conference, which is amazing. Bruce Jennings, James Murray and Kanithia Felder. Many thanks to Melissa Farmer, who is responsible for the stage and most of the logistics. Many thanks to our security team and Mr. William Morgan, in particular, for keeping us all safe and secure.

I'd also like to thank our team of extraordinary honors paralegals: Jonathan Adams, Elaine Meyer, Seth Coburn, Alicia Mazzara and Timothy Hatfield, who have helped keep us all having wireless microphones, name tags and generally making this whole summit work.

C E R T I F I C A T I O N O F R E P O R T E R

TITLE: SPAM SUMMIT: THE NEXT GENERATION OF THREATS AND SOLUTIONS

DATE: JULY 12, 2007

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 and DEPARTMENT OF HEALTH & HUMAN SERVICES to the best of my knowledge and belief.

DATED: JULY 27, 2007

2 C te tracy a fspell th, hyphenation, punctuationelieUTIONS