FEDERAL TRADE COMMISSION

I N D E X

FEDERAL TRADE COMMISSION

In the Matter of:)
CONSUMER INFORMATION SECURITY)
WORKSHOP)
----------)

Tuesday, May 21, 2002

Room 432
Federal Trade Commission
6th Street and Pennsylvania
Avenue, N.W.
Washington, D.C. 20850

The above-entitled workshop resumed at 9:00 a.m.

P R O C E E D I N G S

- - - - -

PANEL V: THE OECD SECURITY REVIEW

MS. COONEY: Good morning. My name is Maureen Cooney. I'm an attorney in the International Division of Consumer Protection here at the FTC. My work focuses on international privacy and security issues, as well as cross border financial fraud.

It is a pleasure for me to introduce to you our panel today on the OECD reform and review of the security guidelines for information systems. In particular, it's a pleasure to be able to introduce to you three heads of delegation to the OECD.

I'd like to begin by introducing Sarah Andrews. Sarah is the Research Director for the Electronic Privacy and Information Center, EPIC, and she heads the delegation that represents civil society. Civil society, in terms of the OECD, is the private sector that is non-commercial. That would be consumer groups, regular users of information systems, educators, and others with an interest, including non-profit interest groups.

Next we have Joe Alhadeff. Joe is the Vice President for Global Public Policy and Chief Privacy Officer of the Oracle Corporation. He also is the head of delegation for global business interests and he does that through the

Business and Industry Advisory Council, which was established to give business policy advice to the OECD and now shares advice in other fora as well.

And finally, it's a great pleasure and with great respect and admiration, I'd like to introduce Commissioner Orson Swindle. Commissioner Swindle is one of the five Commissioners at the Federal Trade Commission. He heads up the U.S. delegation to the OECD's expert group, reviewing the security guidelines.

And all three of our delegates here also have continued their leadership role in a subcommittee at the OECD called the Working Party on Information, Security and Privacy.

Before handing the microphone over today to our panelists, they've asked me to set the stage for you by giving you a little information on the OECD itself and on the original 1992 security guidelines.

Let me begin then quickly with the OECD. OECD stands for the Organization for Economic Cooperation and Development. It is an international group established by treaty by member nations in 1961. Those member nations are the most economically developed in the world and they're what we refer to today as the G20.

Since 1961, the membership in the OECD has increased nearly two-fold. So, there are nearly 40 members

now. There are also non-government organizations that are represented at the OECD. And BIAC, as an example, is a permanent delegate on many of the committees at the OECD, giving business advice.

The purpose for the OECD is really to promote world trade, economic sustainability and fuller employment in member nations and non-member nations, and economic advances in the commercial arena to advance the state of humankind.

To that end, there are several committees and one focuses on computers and communications. That is the Committee for Information, Computer and Communication Policy, the ICCP. That committee, in 1988, determined that they really needed to look at the development of information systems and the security of those systems as more and more people were using computers.

They originally had a staff study commissioned. In 1990, they determined that on the basis of an original report on networks, that they needed to establish an expert committee to give greater policy advice that could be given to governments and to other interest groups to promote security of computer systems and other technologies of communication.

An expert group was finally established in 1991 and at the close of 1992, they issued guidelines. Those guidelines center on nine principles. The principles are an

over-arching umbrella of good policies for security and they're accompanied by approximately 40 pages of explanatory memorandum, explaining what these principles mean, how to implement them. But basically what I would tell you is that the umbrella of 1992 was raising issues rather than necessarily solving problems.

In 1992, the environment was one where there were beginning to be more open networks, but predominantly, the experience of users was on stand-alone computers in closed networks, communications that were open were usually between organizations and their affiliates.

The guidelines are reviewed every five years. In 1997, they were reviewed and the OECD determined that with the advent of wider use of the Internet, there was a concern about open networks and security, but that, at that time, they didn't recommend any changes to the guidelines.

The guidelines were scheduled for review in 2002. In the aftermath of September 11th and in recognition of other global terrorist attacks around the world, the OECD felt it was important to begin a review of security of information systems immediately in order to protect critical infrastructures. And so, there really has been a change in environment.

And with that, I turn it over to our panelists to describe to you their experiences in the review process and

the interests of the groups that they represent.

I give you Sarah Andrews.

MS. ANDREWS: Thank you, Maureen, and thank you to the FTC for organizing this workshop and inviting me here today.

As Maureen said, I work for the Electronic Privacy Information Center. We're a public interest group here in D.C. We are not an official or permanent representative to the OECD. We're merely invited sometimes as observers, other times as participants in the group. But it's in no way a definite that we will be invited to each meeting.

So, we were very pleased to be involved in this process. We were involved in the original 1992 guidelines, so we had some experience in the area and were happy that the OECD invited us back.

In general, we have found the OECD very open to civil society and to the ideas of the non-commercial community, and I think that has helped them be welcomed by the individual and consumer societies and has led to, perhaps, a little less resentment than towards other bodies that are less open, such as the WTO or the World Intellectual Property Organization.

The main issue we were trying to put forward in participating in the guidelines was trying to find a security solution that is workable within a democratic society. So,

security that respects other values in our constitutional democracy. And the OECD generally, in its earlier 1992 guidelines and also in its other guidelines on privacy and cryptography, has, we've found, struck a correct balance between the needs of government, industry and individuals, and this is something we were hoping that they would continue to do.

We generally thought the '92 guidelines were a good document, a workable document, and what we were trying to do was just -- to retain the values and the basic principles in that document while updating it for the current environment. So, there is now, in the document, more of a focus on networks and there's also more of a recognition that computer systems are widely used by ordinary individuals. It's no longer just computer programmers.

And so, security is something really that the average individual needs to be involved with, and we've come up with the term, "the culture of security" to try and represent this, that what we're really trying to get at is the average individual and that this is something for everybody, not just high level technicians.

Some of the principles that we were most interested in -- there were three, I would say. The first was an awareness principle that was in the '92 guidelines and is repeated in the revised guidelines, and this is really a

principle of openness, that individuals can gain access to information about security and can become aware of security.

It's not intended to give individuals access to information that may be proprietary or damaging -- the level of detail that may be damaging about security systems, but that they can have the general comprehension of the processes involved in protecting security and also that there be a general awareness, and there's been a new focus in the revised document of the awareness of risk -- risk to security. So, that's focused more on the average individual, that they know when they're turning on the computer, that there are some risks that they need to be aware of.

The second principle that was focused on was a responsibility principle, so that different stakeholders in the process would know what their responsibilities are, and this may be for providers or security manufacturers, that they have a responsibility to disclose to individuals or to their end users what is in those security systems or new vulnerabilities that may affect those security systems.

But it would also fall back on the individual then if they had been made aware of new vulnerabilities, that they would go ahead and implement patches that were made available to them.

The final principle, and perhaps of greatest importance to us, was the democracy principle and that was in

the '92 guidelines and also featured in the revised guidelines. And this is really the attempt to put security within the context of our society and to recognize the other fundamental principles that are of value to us in society, things like the right to privacy, a right to freedom of movement, free information.

So, the idea that effective security has to take into account other principles, and even though it may lead to an ideally secure society, if we had certain conditions imposed on us, but that we're not willing to give up some freedoms in order to achieve that. So, for example, having everybody chipped -- making those chips trackable so that your location is constantly known to authorities might lead to a more ideal situation, but it would not be something that we're willing to accept.

That is the basic idea we were trying to put forward in the democracy principle, that anything -- it's more focused on governments, when they're coming up with national security solutions, that they really do have to take into account individual rights and freedoms. And we believe that the current draft of the OECD document respects that balance.

That's basically -- that was our input into the process. I would be happy to take your questions afterwards. But otherwise, I will hand over to Joe Alhadeff from Oracle.

MR. ALHADEFF: Thank you. Perhaps one thing I would do, at this point, is to maybe just take a step back so that people can get a gauge of what the guidelines are and what the guidelines aren't, because I think there's some confusion when people look at something that's called security guidelines and they immediately assume that it's something that would tell a security professional what to do in their daily job. That is not and has never been the intent of the guidelines and the OECD is not the place where you should try to draft a document of that nature.

This is a document that attempts to be accessible to all the participants, from the end user to the business person to the technologist, but the technologist would look at this at a very high principle level only because it is not appropriate in this document to get into the granular type of direction that even we were talking about yesterday at what might be basic principles that everyone could agree on in terms of functional things: Oh, yeah, passwords are good, firewalls are good, and all these other kinds of things.

So, it's even a step above that. It's the step of, these are kind of the formative issues that you need to think about that set the framework. From that framework, you then flush out things like these guidelines, like best practices that may exist, and there are plenty of people out there who are already doing those and it doesn't make sense

for the OECD to reinvent the wheel and do it themselves.

When we tackled security at the OECD, one of the things that we were clear about was that security is not a one-size-fits-all solution. There is no one single security thing that you can point to and say, this is the standard that everyone should use. I mean, some people say, oh common criteria is a great standard. Well, sure it is, but, you know, a person who's writing three lines of Basic code at home is not going to run the common criteria on that. QuickBooks is not probably going to run the common criteria. There are just costs and factors that aren't necessary for it to be done.

That companies, who are dealing in very secure products, may decide that that is an option for them is something completely different than saying that that's a standard that applies to all participants. So, again, it's the solution that needs to be tailored to what is appropriate to the system and what are the risks that the system is exposed to, and we won't go into -- there was enough discussion yesterday about what a risk assessment is and whether you should do it and how it plays into the general security hygiene that needs to be developed.

The last thing is there was a lot of discussion yesterday about the concept of passive security, in other words, the security is built in. And I don't mean to get to

the level of discussion where you start talking about whether or not defaults are on or defaults are off or things of that nature. I think the concept, though, is that in order for security to be tailored to a use, there still needs to be some flexibility in the program that allows some levels of user choice.

So, as we have a discussion about the fact that it's great to build security in, you may still want to make sure that security has options in it, because people use things differently. And I think that goes to one of Sarah's points, which is it's important for people to understand what the security functionality is of products as well as what their responsibilities are and what the proper use of that product is. Because you may start using -- you know, there are all different levels, for instance, of digital signatures.

Some of them have very little protection because they're not really meant to be used for highly secure functions. And if someone mistakenly uses it for the wrong function, perhaps they needed more information or perhaps they just disregarded the information they were given. But those are some of the kinds of things where the information is helpful.

We've also mentioned security in the context of the September 11th tragedy, and while that has clearly

heightened awareness related to security, security was not an issue that was created on September 11th of last year. Security is an issue that has been being dealt with by companies, both technology companies and others, for quite a while. Plenty of people could argue that more needs to be done, that it needs to be a broader scope of companies that are involved, that's fine. But security is not an issue that was created on that date.

What was created on that date was an awareness of security at a broader level that did not exist before and that was, perhaps, a benefit that comes out of a horrible event. What was also created was the concept of looking at security in slightly different ways, because before, a lot of people, because of the virus attacks and denial of service attacks, were really just focused on the perimeter. It was just a question of, you know, was it a hardened perimeter, could you prevent people from getting in, but it forgot to focus as much on the people inside.

And you can deploy the best security in the world, but if you've got a clerk who's being paid $6.95 an hour, that's a vulnerability unless you've done some level of vetting and some level of training on that person.

And I will tell you, the worst vulnerability is not the rogue employee who gets bought, it's the employee who really wants to be helpful to the person on the phone. It's

the one who is the biggest subject of social engineering, or what I've called people hacking, which is a person who is just trying to be helpful to the customer. The person is not trying to sell company secrets or divulge anybody's personal information, but the person has not been properly trained in the procedures and is just trying to be helpful, to give the information that's being requested.

That's another issue that needs to be dealt with, and that's part of an awareness raising and a responsibility issue that comes to play.

Awareness raising is different at different levels. It's different at the board level, it's different at the technologist level, it's different at the SME level, it's different at the individual user level. There are other things that you can do in your role as that participant that are not appropriate for other people to do. So, you need to raise awareness for people that is geared to their role.

And the guidelines is a great starting point because it attempts to take a very broad brush at looking at how these awareness issues are set forth. But then it's going to take other people, other organizations, other groups that help make it a little more specific and hang some flesh off those bones, for very tailored communities.

I know the FTC is already thinking of things it can do on the guidelines. The private sector is looking at

things. I would clearly assume that civil society is doing the same thing, and it's going to be a question of how to build upon it. It's not the end. It's, in many ways, the beginning.

And this is something that clearly the industry looks forward -- we heard yesterday about various initiatives that are already going on between the Department of Commerce, Department of Justice on some of these issues.

The other problem is awareness raising needs to be correlated with follow-through. It's nice to raise awareness, but then if no one ever does anything, you haven't improved the security situation in reality. Someone was saying yesterday that, you know, everyone who's gotten hit by a virus has an awareness raising, but the question is, have they done anything as a result of that awareness raising, or are they just going to be susceptible to the next virus?

So, the question is, the education has to be reacting and resulting in behavior modification of some kind that is appropriate to the need of the person. So, those are things where I think you have to -- it can't just be a sound bite, it can't just be a one-shot deal. This has to be more of a campaign that works over time, because, you know, a campaign that just has one shot will not really change behavior. It will make some people think and then they'll walk away, and then by the next time they think about it,

it's not there anymore.

So, industry is interested in looking into how to be a part of that awareness raising, how to help make it go forward, how to provide, you know, better basic information, if necessary.

Business also, of course -- and one of the things I wanted to highlight, which was an issue that was brought up yesterday, and it relates to training and awareness raising, is the concept that while we may train people on security and often that training deals with, you know, how to deploy your virus protection, how to make sure you're using a firewall, you don't have ports open on your servers and all these other kind of things, that's fine. But often it's training that we forgot to do related to, can employees even recognize when a breach is underway.

In a large company, you may not need that as much because you may have deployed intrusion detection systems, you may have appropriate traffic management systems that can look at those patterns and try to look at those issues. But in smaller companies, there are sometimes tell-tale signs, whether it's system slowdown, whether it's certain types of errors that get generated, that aren't just a glitch. They're a sign of something going on. And have we heightened awareness sufficiently for those people to take those things seriously and not wait until they can actually find the

damage before they react to them?

So, again, those are things that -- it's starting to think slightly different. Training, up until now, has been kind of the functions of security and how to do them. It hasn't been how to secure and protect the environment as much. So, I think you'll see some shifts in the way some people are training on these issues as well.

There are some concerns, clearly one concern which goes on the concept of there is no single solution, you always want to retain the flexibility to deploy the appropriate solutions for your needs. So, there's still a concept that you don't want to see legislation that's technology specific or things of that nature. Those are not appropriate. You need to have appropriate flexibility and awareness to develop policies, practices and procedures.

And when you look at security, this is -- you know, often people just assume that security is a technology deployment and perhaps a security policy that goes with it. And there's a lot of focus on authentication, you know, how you know the person coming into your system is the right person. And all that's fine and that's all necessary.

But there are other things that people also don't -- sometimes don't pick up on, and that is, well, I've authenticated the person, but beyond that, I also need to make sure that I have personnel policies, that I make sure

that the privileges are kept up-to-date because I could authenticate a person that's no longer working for the company because someone forgot to update the privileges.

So, it's a whole systematic concept. It works throughout the entire company. It works across a number of policies, and many of them aren't called security policies. Some of them are called personnel policies, some of them may be called privacy policies, some of them may be called net use and access policies. There may be lots of things in there that don't fall under a direct rubric of what we would consider to be a security policy, but are likewise -- but are still very important things.

Another thing which is a big item, which has been much more highlighted in this set of guidelines, is the concept of the sharing of information. In the United States, we have the ISAC as one of the ways in which information is shared.

And there are some issues that have arisen even around the ISAC creation, which are also relevant in the OECD context, and that is making sure that the sharing of information can be appropriate to make sure that you are not actually compromising security by sharing the information, to make sure that the information, if necessary, needs to be kept confidential and to make sure that the information is treated in a fashion that benefits security.

So, all these things are factors that, again, retain the flexibility and, I guess, the concept of appropriateness of the sharing and the voluntary nature of the sharing is an important factor to keep in mind.

The last thing, perhaps, is also a concept related to law enforcement. We saw with the I Love You virus that it originated from a jurisdiction that did not have a statute on the books that would make it possible to go after the person there.

So, while there are some issues related to law enforcement, where it's clearly within the purview of law enforcement to figure out how best to have a process to inter-relate with law enforcement with other jurisdictions, there needs to be a mechanism so that if someone in one country is suffering an attack from outside of their borders, across the Internet, that there is a way to reach out to your own law enforcement and have them coordinate appropriately with law enforcement in other countries.

And that's not really something that was dealt with within the guidelines, because that's really something that the G8 is working on, and it was, again, really not the intent of the guidelines, which were focused much more on some of the economic security issues than on the major critical infrastructure issues.

But those are all factors that have to come into

play and all factors that you have to figure out how they are going to work and how they are going to move forward, because it's -- the one thing that the guidelines try to highlight, and the one major change from when Maureen introduced the '92 guidelines, which were really guidelines that, while they mentioned networks, really focused on insular systems.

And in many ways, the reason that in '97, at the review there was a decision not to do anything, while there was an Internet, it really was just like a really big insular system, and people weren't really thinking of it in the robust terms of how we think of the Internet today. And so, that's why while there was a concern, there wasn't a decision for action at that point.

And what ends up happening is, now, you really do have to pay a much larger focus on what's happening to systems outside of your own. Threats may originate from there, damage may result to there. Both of those things need to factor into the way you look at your system, and one of the things that these OECD guidelines do is to create a much more holistic approach so that people think of themselves as an interconnected part of a system and not just as the little island. Because as the little island, you will not see half the risk or even a portion of the risk that you are exposed to. You will just see yourself as the island.

And the challenge becomes how to make that

information appropriate and intelligible to the various levels of islands. It's one thing to make it intelligible to an enterprise, it's another thing to make it intelligible to an individual. And that's one of the challenges that faces what I would call the progeny of the guidelines or what you do after the guidelines, because there's no way that one document can get to that level of explanation for each of the participants.

It has done -- it has been a valiant effort to get the document to be as relevant to as many participants as possible, but one of the things that people are going to have to figure out is, how does my island relate to the larger archipelago, if not the entire map? And, you know, that's -- I guess today we're going to do maybe the island analogy instead of the car analogy.

But that's one of the big questions that this is trying to get at, that this isn't isolated. At the company level, it's trying to tell you, it's not just your IT department that has to worry about this issue. For too long in companies, security was thought of as the guy with the badge downstairs who looked at your ID, and now, security has a much larger ethos.

I was recently visiting a friend in a hospital and in hospitals now they have all sorts of signs in elevators talking about don't talk about patient information in the

elevator. Lots of things are being thought about now, which weren't thought about, which are being disseminated to the broader populace, within companies, with the broader user population up at the board level. It's much more pervasive now. And, again, that may be an unfortunate result of September 11th raising the profile.

But this is an issue that is much more fundamental than September 11th. It is not a September 11th solely related issue. The fact that awareness has been heightened should not make us think that this needs to be part of behavior, and therefore, I guess, that would be my closing comment and I'll turn it over to the Commissioner.

COMMISSIONER SWINDLE: Thank you, Joe. Yesterday, someone was talking about the use of computers and how they've grown. I must reflect back to my Marine Corps career. My final assignment in the Marine Corps, I was a general staff officer for finance for a logistics system. I was a Marine aviator assigned to that task and it made it somewhat unique in perspective for all those people who weren't Naval aviators because we do things slightly different, and I was a little bit of a shock to the system.

But one of the shocks that I imparted on the system -- it took me four years to do this -- I got there and I had roughly 100 people working for me and we were taking care of all the accounting for our entire logistics system,

which is huge. It's $3 or $4 billion as I recall back on those days. And we were doing it all with adding machines -- they were electric adding machines -- no, some of them were -- they had those, you know, (making noise) thing like this. This is the late seventies. And we were pushing pencils on big sheets -- accounting sheets, which I just get prickly when I think about those things because I never liked accounting in college, but here I was in charge of it all.

And I said, surely there's a way to do this differently and I started asking about computers because I didn't know anything about computers, and I quickly learned that we had a central computer function in the command. It was called the computer center and it was air-conditioned to the hilt, it was bright and shiny and had those boxes that whirl all the time. It was like a sterile operating room. And I wasn't allowed to go in that room. The computer people were allowed to go in.

They had a Colonel and I was just a Lieutenant Colonel, and the Colonel would come to the staff meetings every week and he was different from everybody else. He was sort of a nerd, if you will, and I kept wanting to know how everything worked, and we were using the little -- the computer cards that we all learned how to -- those of you who aren't old enough, you probably don't remember. But these cards, and we had time cards that people had to punch clocks

and all that. It was the most mechanical bizarre thing, and we'd all put this input in through these methods, these cards, every week. And then the big computer, over the weekend, would run. And then on Monday, it would spit this stuff out.

And I said, this is nuts. As you -- those of you who have come to know me, I tend to try to simplify things. So, I was trying to simplify this, and I said, I've heard of something called a mini-computer. Does anybody here remember mini-computers? Now, that's different from a PC, I think. I'm not very intelligent about all this stuff. But I said, I want some of those mini-computers, whatever they are, they sound good to me.

Oh, well, you can't have those. I said, what do you mean I can't have them? Well, there was a law -- there was a regulation or a policy, I guess is the proper word, in the Department of Defense that says, we will not allow the proliferation of computers, all sorts of things bad would happen. Well, I think we've made it. They were right.

Interestingly, I set out on a crusade, just a personal crusade. I'd come up here to Washington -- I was down at the Logistics Center in Albany, Georgia. I'd come up here to Washington about once every quarter and I'd go over and talk to a good friend of mine, a civilian in the Marine Corps, a GS-SES or something like that, and I'd say, Gene, I

want some mini-computers, show me one. And lo and behold, at headquarters, he had one. I said, now I've broken the code. Certain people can have mini-computers, but the guys in the computer center won't let us in.

And so, the day I retired from the Marine Corps and left that command, of course, we received word that we were getting mini-computers for my financial management division or the comptroller's, we call them, and that began the downhill slide. Now, we're all involved in these things and it's just fascinating what it's done. It's made things far more efficient. It's made things far more fun. And with the advent or the public awareness of the Internet, as Joe said, it's been around substantially longer than 1992 when Netscape hit the scenes and whatever that proper date would be.

But it's made the world far more fast, far more vast, far more fun, and we just charged out just new innovations, gimmicks, gadgets, and, you know, we got way out there. And as we charge forward, it's like -- it's like Patton in Europe. He got so far ahead of his logistics and the rest of the lines, he was way out here, a salient point, and guess what, he became vulnerable along the sides. And we sort of are there now. We've gone so fast, so far in all these advancements, in all the fun of it, that we forgot to take care of security in its entirety.

Companies are very much aware of this. They have proprietary information. They have information about customers they'd like to protect, confidential. So, they've taken some steps along the way, but nobody thought about the consumers.

And so, the Federal Trade Commission, since we think about consumers, we thought it appropriate that perhaps I could sit on the expert group in the United States and the revision of the OECD guidelines.

By the way, Sarah mentioned that EPIC is not a standing member of this -- the WISP and all these acronyms that I've come to know. If I have anything to do with it, she will be a permanent member because she's made a heck of a contribution to the effort over there. Joe Alhadeff has made a tremendous contribution. The members from the various countries have made tremendous contributions, and I'll talk about that shortly.

But we've had people involved from Treasury and Commerce. I think I saw Helen Schull (phonetic) in the audience. I can't see her -- hi, Helen. But we've had just a superb group from the U.S. Government involved in this process and I think everybody's had a chance to make a contribution. We've had Treasury, State, Commerce, the FTC and Justice Department. I may have left somebody out, but I think that's most of them.

I went to the first meeting in December. I walked into a whole new world. I heard terms -- Joe used one -- we haven't used that word in several meetings. He talked about granular. I'm looking around and I said, what does that mean, you know. And fora is another word. At Georgia Tech, we didn't teach these words. And civil society, I had never heard that term before. So, it was all a real experience to me. But I sat in the first meeting, and it happened to be held over at the State Department -- the meetings got much better, we went to Australia and then to Paris.

But have you been in the State Department lately? I don't know anybody at the State Department, and I think it's for good reason. I don't like to go in their building because they check everything. Talk about security conscious.

But when I went to the first meeting, I listened, and many of the people who were attending had been involved in the '92 guidelines. So, I'm really the new guy on the block, but I'm listening to what's going on. And as I think Joe, or Maureen perhaps, indicated, the meeting was a follow-up on a meeting in September. It happened to coincide, as I understand it, September 12th in Japan, which was September 11th here, and they said, we've got to look at these security guidelines and revise them and get them up-to-date because they were essentially developed before the real presence of

the Internet.

So, I'm sitting there listening to a bunch of experts who were real familiar with this process, and I didn't know anything about it. But I made several points when I got my chance to speak, which some would observe was more frequent than it ought to be. But that's my nature.

I made some observations, and I was looking at the document and I was listening to the words and the words didn't sound very user-friendly. They sounded very bureaucratic. The OECD is a grand concept and it's done some marvelous work. But it does tend to be a wee bit bureaucratic, somewhat like the Department of Commerce, Helen, where I was, which is a monstrosity of a bureaucracy, surpassed only by the Department of Defense.

But anyway, I said, some points I would like to make as we go forward. First, it needs to be user-friendly. That means plain English, and then I found out that that's not an appropriate term to use when you're in an international audience. So, I had to say plain Japanese, plain Russian, plain Norwegian and so forth.

Interestingly, I heard the conversation as it went and there was something we got in a huge conversation about called the explanatory memorandum. And I asked a relatively stupid question; I said, if you've done a good job in coming up with nine principles, guidelines, then why do you need an

explanatory memorandum? Then I was completely appalled when I found out that the principles occupied about one page, maybe two, and the explanatory memorandum occupied about 17 or 18, if I remember correctly. I said, we've got a problem.

So, I said, we need to get this things squeezed down. It has to be brief. It has to be in plain English. I'm pleased to say that the current edition, which is not totally finalized -- it should be within another month or so -- has no explanatory memorandum, and instead of being 49 pages long in its officially published form, it will probably be about -- maybe about 10 pages long.

And we were talking about timeliness and we were shooting for a target of having these revised guidelines out by May of 2003, and my mind doesn't work like that. That's like being out in the Pacific where you're told -- I spent a lot of time in the islands and they said, there's two kinds of time out there, there's now and there's not now. And OECD is caught somewhere in between that.

So, we're going to get these things out by this September, which I thought was sort of an appropriate thing. And all that's well and good. That's a matter of ginning up a bureaucratic process and making people really focus and work and try to hammer this thing out and get it done, and I am -- I just really admire the group that's been working on this, especially the ones in the United States who have made

just a tremendous contribution, these two folks and our U.S. Government team. But everybody's made a contribution.

But that's the easy part. The hard part is the implementation and how we -- you know, the devils in the details. How do we take a bureaucratic document -- and it still is -- that is somewhat cold, it's not the Magna Carta, and how do we develop it into a story that is easily understood, easily disseminated, easily used as a basis for implementing something that will create, the term that is used here, create a culture of security, a new way of thinking, if you will?

I likened it in that first meeting -- again, being overly simplistic I said, for God's sake, what we're really talking about, and get away from these huge words and these huge concepts and get it right down to what we're talking about. In security of information systems and network, we've gone from the vertical stovepipe kinds of things to this interlocking thing, and now, everybody's involved in it.

And I said, and when you talk about consumers -- you remember Richard Clarke used the hierarchy, national security, global security, national -- and you got down to the bottom tier and it was consumers and home users and small businesses. That's where everybody is. That pyramid is like this and it narrows down to this and the attention's been up here, somewhat

adequately, not totally obviously. But down here, nobody's thought about it.

So, how do we create a culture of security out here? And I said, it's got to be so imbued in us, it's got to be so intuitive that it's like me crossing Pennsylvania Avenue -- and I told the now too often told or related -- I'm really having an effect because somebody used it yesterday. I said, it's like me the first time I was ever taken to school as a six-year-old. I was walked to school, a small town, no stop lights, but we had crossroads. And I was told by my grandmother, when you get to this street, you stop and you look to the left and you look to the right and then you cross the street.

And I said, to this day -- she didn't write that down for me because I didn't know how to read. But to this day, when I walk across this street or any other, I look to the left and right. It's intuitive in my -- it's a way of thinking, and that's what we have to achieve in this process.

We've got to tell a story. I think President Bush has done a good job of alerting the general population to the fact that we're all involved in this. We're sitting at home now -- youngsters, someone mentioned a three-year-old -- with computers that someone has told me, who knows far more about this than I do -- and I still don't believe this -- but he said, to make an analogy and make a point, that the computers

we often have at home, are more powerful than the computers we had on some of the first Space Shuttles, certainly some of the first space capsules. That's staggering.

And they're all inter-connected. A three-year-old, in a sense, in reality, because of the power of that computer and the inter-connected nature of the Internet is linked up to the California power grid or the air control system or to NASA or how about to the Defense Department, and lo and behold, it wouldn't surprise me if they're not hooked into the primary intelligence gathering systems over at the FBI. They seem to be having a problem.

So, the point is, we're all involved. And so, the point of the guidelines was to -- we wanted to get across to everybody that you're involved. Joe used the term "participants." We struggle -- I have a lot of little simplistic things that I get upset by and I cannot stand the word "stakeholder." So, if you ever come to my office on official business, don't ever use the word "stakeholder."

And so, we no longer use stakeholder. Stakeholder was throughout this thing. It was like, you know, going to Outback, you know, it's some stakeholder, stakeholder.

(Laughter.)

COMMISSIONER SWINDLE: And so, we -- as Joe said, we have to write up something here that's applicable to that three-year-old, in a sense -- that may be stretching it too

far -- and Bill Gates sitting at Microsoft. And I think we've come close. As I said, this document is not the Magna Carta. So, don't get all excited in anticipation that it's coming.

What it is is a boiling down of some basic ideas, and among those basic ideas are common sense things. In fact, I made the point that if we came out with them and everybody looked and said, eh, we might have achieved what we were setting about to do. That they would be intuitive. And some of it's not quite so intuitive because we had to deal with the technology that Joe so eloquently spoke of a while ago.

How do you incorporate what he just said to where somebody like me can understand it? Tough job, 30 countries have been working on this, 30 plus countries, a small group of experts. I find it humorous that I'm in that group. It's almost as humorous as me going and talking before a bunch of lawyers and all of them taking notes for their continuing legal education. This is really something, guys.

(Laughter.)

COMMISSIONER SWINDLE: Anyway, I think Dick Clarke was right on target. I'll summarize the whole conference here this afternoon. But prevalent in this always are the tensions between privacy and security, and that's why we need Sarah and EPIC and people from the civil society, that's why

we need Joe Alhadeff and the business community, and that's why you need government. Because all of us represent a point of view and the best solution we're going to come out with, because we are this pluralistic society and we are a democracy, the best solution we're going to find is going to come from these three groups -- and there are others -- constantly pinging at each other, trying to hammer it out to make sure we're covering everything as best we possibly can.

And I heard the term used a couple of times yesterday, we're going to "ensure security." Don't you believe it. We can't ensure total security. We're going to get close, but we're not going to achieve perfection. And I think we've done a good job.

The last point, as I said, the tough part of this is implementation. It's an enormous task. I think it was Mary Culnan yesterday said, there has never been an outreach program that got to everybody and that's -- not even close to everybody. There's never been this huge grandiose outreach program. But if we're to have a culture of security, if this is to be intuitive in our thinking, we literally have to start with the generation just starting to use computers and keep preaching it, teaching it, showing them the way.

I always get a kick out of some of the commercials. I think Dell, who I happen to have great respect for as a company and certainly their equipment. They

used to have a commercial where they showed this cart being rolled into the classroom and all the little kiddies jumping around. They're all going to get a $3,000 laptop and sit down and destroy the world. And they were teaching them how to use computers and the fun of it and the education value of these tremendous things. And I wonder if they ever thought to teach them about the security implications of being on the Internet with that powerful tool.

That's what we've got to convey. It's going to take time. It's going to take a lot of education. And I've talked too long. But it's going to take -- importantly, this is the most important thing about the implementation thing. It's going to take every single one of you in your different roles in the environment to help us cascade, if you will. This is going to be poured out from the top, nine principles of the OECD. Like I said, don't get real excited that the Magna Carta is about to roll out of Paris, because it is not.

But if we can take the principles in it and put them into a story that is sophisticated enough for Oracle's entire organization and is -- I don't mean to use this term in the wrong way -- is simple enough to be taught to kids in the fifth grade who are learning how to use computers, and everybody in between to make these points that security is important, that we're all players, whether we want to be or not. We are all interlinked together. We are all terribly

reliant upon each other, and what we do has the capacity to hurt ourselves, but even more important, hurt other people. And that's what we're driving for and that's what we've been trying to get.

Maureen?

MS. COONEY: Very good, thank you. We have a little time for questions. So, if any of you would like to approach the microphone, please do so now.

Maybe I would begin and -- since we have a limited amount of time, I'll just ask two questions. One is I want to make sure that this group has a clear sense of what the principles, as they're being rolled out, look like now. And I was wondering if, perhaps, Joe Alhadeff or Commissioner Swindle would address the shift in the types of principles and the security life cycle concept.

MR. ALHADEFF: Sure. The principles previously were all really what you would consider to be general policy principles at the highest level. And while the level really hasn't changed, what has changed is perhaps the first five principles remain more of these general application policy principles, and the last four have shifted to a more operational sense, that is attempting to reflect concepts inherent in the security life cycle, and I don't mean the product life cycle, but I mean kind of the security life cycle of things that you do in terms of security.

I don't really want to get into a lot more detail because the OECD frowns upon you disclosing draft documents until they are beyond draft form. So -- but that is the structural component shift that has been -- and there was also a shift, which I think we have to thank the Commissioner directly for, because you had principles before that were called multi-disciplinary principles, which even to those of us who are schooled in OECD speak meant absolutely nothing.

So, he has forced me to take a lot of words out of the lexicon in terms of I'm not allowed to use granular or egregious, which are two of my favorites.

COMMISSIONER SWINDLE: I'm dumbing down the whole group is what it amounts to.

MR. ALHADEFF: Actually, it was a refreshing change in the sense that someone who hadn't kind of participated in the pre-OECD functions came in and said, you know, what's the purpose of the document, who's going to read it and why are we drafting it. Somehow, those questions we forgot to ask along the way usually. So, I think the document has a greater accessibility. And I'll be quiet so other people can ask questions.

MS. CARLSON: I'll just address this question to you, also. You had mentioned that technology specific legislation is not a good idea. Last week, the Senate Commerce Committee passed a bill that's mostly focused on

cyber-security research and development, but it has a provision that would give the government the authority to create kind of a baseline security configuration. Could you comment on that and where you'd like to see it go?

MR. ALHADEFF: Yeah. I think we -- there has been this concept of technology neutrality that's been around for quite a while. And the problem is, technology neutrality has gained such a mantra and life of its own that it almost became to the point where you were asking the government to create something completely functionless, too, at the end of the day.

The concept is that you shouldn't be choosing, necessarily, a specific technology if a number of technologies can do it. If it's a neutral standard, it's based on consensus principles, it's market available, those kinds of issues are what you need to do. You can't just be wink, wink, nudge, nudge, that one. And that's what you have to stay away from.

There are -- there were digital signature standards in Germany, for instance, which kind of said -- really had picked one company as the winner at the end of the day on that score, and that, you can't really have. So, perhaps it's not the breadth of technology neutrality that we once said, but it does have to be kind of a neutral set of playing field principles that, you know, you're always going

to have requirements for something that are creative, and it's not a problem that you create requirements as long as they're open based on needs and principles and reflect kind of an even playing field.

MS. CARLSON: Do you support that legislation?

MR. ALHADEFF: In all honesty, I've been wrapped up in this and a couple of other issues, so without reading it, I can't tell you whether I support it or not.

COMMISSIONER SWINDLE: If I could comment without going specifically to that legislation before the Congress. There are numerous of these things that deal with everything from privacy to security and identity theft and SPAM and there are a lot of things being considered. We've been in this discussion on privacy now seriously, I mean, for the last 10 years and it's been going on since the 1970s. I can recall one document.

But here -- I'm going back to this concept of what a democracy is all about, and that's all of us having a say in the process and the dialogue, as I tend to call it. I am convinced, and I have said it until I'm blue in the face and some people have listened, but I don't think any of these problems, be it privacy or security, can be solved by a new law or a new regulation, or even a new law enforcement activity, which we're setting about to have lots of new law enforcement activities, and that's good. But it's going to

take a combination of all of that.

The private sector, it's been said by people far brighter than I, owns about 90 percent of information technology, the Internet and everything associated with it. I'm finding that this thing we're talking about includes everything in the world, it seems. But the private sector has or should have the truest of all motivations to get it done, and I think the private sector has done a good job in advancing both privacy and security.

Is it perfect? Absolutely not. Do we have work to do? Yes. It's like Robert Frost said. We have miles to go before we sleep. But I'm convinced if we'll just keep talking and keep debating the issues and keep challenging, at the end of the day, we're going to come out with whatever -- with the best possible solution of these very complex things than we would if we just, all of a sudden, hear in election year "and we want to do this," pass new laws and everybody sit back and say, well, we've solved that problem, let's go find something new to do. The progress will stop.

So, that's what we're up against and it's going to take all of us working on it. And you folks in the media, in particular, keeping the pressure on those of us in industry and in government who have a responsibility to get this thing done. If the private sector doesn't do it, the government is going to do it and we'll be lesser for it. Thank you.

THE REPORTER: Ma'am, before you leave, could you identify yourself for the record?

MS. CARLSON: Yes. My name is Arlene Carlson (phonetic). I'm with eWeek (phonetic).

THE REPORTER: If anyone who has questions, would they identify themselves for the record.

COMMISSIONER SWINDLE: This guy coming up is living under an assumed name.

(Laughter.)

COMMISSIONER SWINDLE: So, disregard anything he says and bleep this out of the record.

MR. LANE: Today I'm going by Terry Lane. I'm with Washington Internet Daily. You talked about the OECD guidelines being a simple, readable document. Is it going to be detailed enough to where any, say, government agencies or any government around the world who might want to use it as a basis for any type of regulation or rule-making to compel some industries to adopt security guidelines, would it be detailed enough to facilitate that use?

COMMISSIONER SWINDLE: I'll speak briefly. I think if they are sound principles, and I think they've been well thought out, given what we're up against, we're dealing with different cultures -- at least 20 different cultures, I'm grouping the Europeans together and saying they're all one, which we all know is not true -- and different

languages. We spent days -- certainly a number of hours talking about -- I think the word was comprehensive, and at the end of the day, the Japanese informed us that -- I think this is the word -- that they don't have a word to translate into that. So, we spent hours and there's that kind of problem.

But I think if we do, in fact, arrive at principles, principles last for a long time. Our Constitution is filled with principles, and if we can arrive at principles, then different societies should be able to take the essence of the principle and, indeed, use it as a model, if they choose.

But one thing that I don't know if Maureen mentioned, but OECD and what it does has no obligation whatsoever on anybody, and we make that point. That's plainly stated. So, I think there will be good models for those who want to do it, but it will be up to each country to implement them as they want.

Sarah, you and Joe weigh in on that because you've got more experience with this than I have.

MS. ANDREWS: I think that's right, that these are intended to be high level principles that different countries would use in different ways and may form the basis of legislation. And it's consistent with other guidelines coming from the OECD, such as the 1980 privacy guidelines or

the 1997 cryptography guidelines. They just set out some basic standards, but not prescriptive.

MR. LANE: Have the privacy guidelines been used for legislation -- as the basis for legislation in other countries?

MS. ANDREWS: Very much so, yes.

COMMISSIONER SWINDLE: I want to make a point to my media friends. When I say this is not the Magna Carta, I'm not slighting it. I'm just saying it's a document that evolves out of a complex organization with 30-plus views. To an American, that might not appear as something we can get real excited about. But if we've done a good job with the principles, there's a message in there.

As I said, there's a story in there that imparts a new way of thinking. And if we can get that across to the people of our society, and other countries can do similar things in whatever way they choose to do it, because we'll all do it slightly different, then we've gone a long way to shoring up this concept of a culture of security.

MR. ALHADEFF: And I'll add to that, that what it really does is it gives you a framework for thinking about the issues. Whether you think about them -- I mean, it's not presumed that legislation will flow out of it. It's not presumed that any specific thing flows out of it, but it gives you a context for how to think about some of these

things and raises issues that are of substantial importance to security. How you use them then will depend upon your situation.

So, I don't think we can predict how they will be used or how people will find them to be useful. But the concept was they should be useful to a broad range of participants and the government was clearly included as one of the participants to whom it should be useful.

MS. COONEY: Okay. Do we have any more questions from the audience?

(No response.)

MS. COONEY: With that, I'd like to thank our panelists very much.

(Applause.)

(End of Panel V discussion.)

PANEL VI: EMERGING STANDARDS FOR BUSINESS SECURITY

MS. FINN: My name is Ellen Finn. I'm an attorney in the Division of Financial Practices in the Bureau of Consumer Protection here at the FTC. And this panel, we're going to be talking about emerging standards for business security and those standards may emerge from a variety of places and that's one of the things we'll talk about today.

Some of the discussion actually started a little bit yesterday, for those of you who were here. But we're going to focus in more depth on a variety of developments that may drive towards different kinds of standards for how businesses secure information.

Again, there are detailed bios for all of the panelists in your materials, so I'm just going to give very, very brief introductions, and I'm just going to go down the line alphabetically and let everybody make a brief presentation. Then we'll have moderated discussion and we'll accept questions from the audience in about the last 15 minutes of the panel.

We'll start first with Kimberly Kiefer. She's

currently the sole proprietor for the Center for Security Law and she practices in the areas of intellectual property and computer and Internet law.

MS. KIEFER: Okay, thanks very much and thanks for having me today.

I'm with the Center for Security Law, but that's kind of just a cover for the past couple months where I've been writing some articles and working a lot with the Committee before I move on to transitioning into the Department of Justice, Computer Crime Division, moving from information security over to the law Enforcement side.

I'm very excited to be here because the past six months I've been working on two separate initiatives in the area of evolving standards and gotten involved with lots and lots of discussions with technologists and lawyers about what we can do, what we need to do, and I'll just dive right into it.

The first is an article I'm working on with Randy Sebett (phonetic) from Cooley, Godward. He is either an associate or a partner over there, and we have a forthcoming article, most likely in the BNA Electronic Commerce Law Report in the next couple of weeks, another form of that article in the Information Security Magazine in September. They have a new publication for chief information security officers coming out. There will also be another form of the

article in a law review coming this fall.

What that -- that article is called Information Security Liability: The Developing Legal Landscape. And it goes into many different types of liability, focusing on that for organizations operating on the Internet, rather than network or ISPs or software vendors, technology providers. Most of the articles now are focusing on those two parties.

And what we get into -- we get quite a bit into the negligence area and come up with a list of standards, 22 -- it will probably go up to 25 by the time it's published -- standards for organizations operating on the Internet, divided into compliance standards, process standards, policies and technologies. Based on quite a bit of work with the group of CISSPs and -- that's the certification for information systems security practitioners -- both Randy and I are certified with that group, lots of conversations back and forth on what the standards should be really from the technological area.

So, we're excited about that. And the point there is that liability is no longer a question of if you have liability, but when the cases are going to happen and how you can protect yourself before that happens.

The second thing I want to talk about briefly is my work with the ABA Information Security Committee. It's a committee of 400 now, 400-plus, lawyers and technologists, a

section of science and technology law with the ABA. The committee is responsible for drafting the digital signature guidelines, which received international recognition in 1996 and then the PKI assessment guidelines, a 400-page document on assessing public key infrastructures that recently came out. It's going to be finalized in the next couple weeks.

Our next project, of which we have a -- almost a second draft and hope to have published by the end of the next month is called an Information Security Legal Manual. And the idea is to address the corporate management and legal counsel on what you need to do with security.

One incident -- a couple incidents I always give is when I was working at my last law firm, talking with clients who had called me up after security breaches had occurred, one said, what should we do, what should we do. And I said, why don't you just take a step back and tell me what your incident response plan says and what -- and they said, what's that.

So, this manual is very much addressed to corporate management, what they need to do. It's a reference manual that will sit on your desk that explains information security to you, potential liability, and most important for this panel, it has a list of standards as Appendix A, divided between systems -- systems standards, products standards. It categorizes them into five or six different categories and

gives an explanation of them, which is kind of a nice area to be able to turn when you're first coming into this area and looking at standards.

So, as far as standards go, and this is what the article gets at, and bringing in what Commissioner Swindle talked about, is that there's a lot of disagreement over whether such standards are possible, differing needs of organizations and how do you -- with the changes in technologies. But the standards are derived from the idea that there are commonly accepted security principles that perpetuate regardless of changes in technology and regardless of business needs, and these standards can be promoted to all organizations.

Some legal scholars say that companies must -- and people in the information security industry say, companies must implement these, but we set -- what we talk about in both the manual and the article is that companies must consider these and implement if appropriate.

Last, what I want to leave with is a quote from a case, one of the first cases that dealt with landlord/tenant liability and obligated the landlord to install certain security measures in common hallways. It was a tort liability case and it's been used to -- as an analogy for why certain organizations operating on the Internet may suffer from tort negligence liability.

But what the judge said in this case was, "In the fight against crime, the police are not expected to do it all. Every segment of society has an obligation to aid in law enforcement and minimize opportunities for crime." And in that regard, as far as keys to security, I'd like to leave you with five -- five brief steps on how we can have more security in society.

The first is, safe computing practices from customers, which we talked about yesterday; best practices standards for organizations operating on the Internet, which are the standards we'll be talking about today, as well as the ones I mentioned in the article; secure coding practices for software vendors; increased education of the young people today, that hacking is not acceptable, it's a crime; and increased prosecution of these individuals; and last, enforcing liability.

Thank you.

MS. FINN: Thank you. Next up we're going to have Peggy Lipps. She's the Senior Director for Security and Risk Assessment at BITS, which is the technology group for the Financial Services Roundtable.

MS. LIPPS: Thank you, Ellen, and thanks to the FTC for hosting this workshop.

We're very excited to have an opportunity to tell you a little bit about BITS and what we do. BITS is -- it

actually used to be the Banking Industry Technology Secretariat. It is no longer an acronym because our members are not just commercial banks, they're insurance companies and brokerages as well, so integrated financial services, across the board, as a result of the Financial Modernization Act.

But BITS was actually created by the Financial Services Roundtable, which is a traditional lobbying organization whose membership is open to 100 of the top 150 integrated financial services companies by market cap. BITS was formed by the CEOs to focus on issues of e-commerce, emerging e-commerce, payment systems technologies, to facilitate the growth of financial services, but also while ensuring that safety, security and reliability of service was maintained to the consumer.

So, our focus, primarily, it's in the area of criteria development. They're essentially voluntary guidelines. Our work takes a number of different shapes, actually, but that's probably the core of what we do and our members tend to focus on areas that are not considered competitive. We really have a strong, you know, secure-as-the-weakest-link philosophy, and so, if all of our members are not up to the same level of security guidelines, the concern is that we could all be negatively impacted.

In that philosophy, BITS also opens its membership

to other associations like America's Community Bankers, the Independent Community Bankers Association, the American Bankers Association, the other ABA, so that the work that we do gets the broadest reach within the financial services industry.

But to give you a couple of examples of the security standards type of work that we do, one is in the framework that we developed for managing third party service provider relationships. Obviously, our industry has a heavy reliance on third parties and making sure that the appropriate control requirements are in place for those third parties is critical.

Another -- on the other end of the spectrum, considered, perhaps less voluntarily, for those who choose to go through this process, we have a BITS product certification offering, which is security criteria that's been developed by the Financial Services members, upon which a security vendor's, or any kind of e-commerce vendor, technology is tested.

In the event that the vendor meets the criteria that's been established, they're actually issued a BITS tested mark. So, they actually get a seal of approval. Again, it's against, though, criteria that's been developed by Financial Services and, of course, those that purchase the products are not required to purchase products with seals.

Some examples, though, of the kind of criteria, the third party service provider framework that I mentioned would cover areas such as when to engage or how to determine whether to engage with a third party service provider, what you should consider in the RFP process, what kind of contractual considerations should there be, what type of control requirements would you want to consider to have in place; what do you need to consider in terms of the implementation and the conversion of that service, and then, finally, considerations in the ongoing relationship management. On the -- again, as it relates to security and privacy of the services that you're getting from those third parties.

On the other side, on the product side, the criteria would look at identification issues, authentication, authorization, data storage, confidentiality of data, all those types of areas, and would define a minimum requirement that the financial services industry considered.

The primary drivers of the work that we do, sometimes it is driven by regulation that's already out there. Again, as in the example with the IT service provider document. But other times, it is driven just by the fact that there's a new technology and in order to deliver its -- that technology and services on that technology safely to the consumer, we have to define the criteria on our own and drive

the market.

In that case, some examples are our mobile financial services guidelines that we've developed for the wireless area. And in another case, the aggregation services that many of you may be familiar with, and that's where a consumer looks at all of their financial information online in one location. In both of these cases, there was not any kind of regulation that preceded us. But we'd like to think and we hope that, to some extent, we help to shape that regulation potentially.

And I would say that most of our criteria is generalizable beyond financial services. One of the alliances that we have -- strategic alliances with the Department of Navy, and they came to us because they felt that the criteria was very strong, that the financial services industry would produce, they were buying a lot of off-the-shelf products and services, and so they've continued to work with us as our criteria development efforts evolve.

The success of our criteria is based on two things primarily. One is that we use a very collaborative approach. I did mention that we involve other associations in our work, but we also involve any of the -- I will say affected participants as opposed to stakeholders. But oftentimes, the government regulators, the security agencies, we -- in all of the criteria that I mentioned, we invite the technology

providers that are involved, the third party service providers, so that we can get the perspective of all that are affected.

While the financial services industry develops the baseline document, it does get modified through that whole process and ultimately we do put all of our criteria out on the Web site and make it publicly available.

The other reason why we're successful, I think, is because we are CEO driven, and when we produce our criteria, it is approved by our boards, the Roundtable and the BITS board. Again, it's all voluntary whether the financial institution chooses to use it. However, the fact that it has gone through that consensus building process and involved so many of the participants does impact, I think, the success.

Hopefully, that gives you sort of a snapshot into what we do and I look forward to the panel discussion.

MS. FINN: Thank you. Next we will hear from Mark MacCarthy, who is the Senior Vice President of Public Policy for Visa, U.S.A.

MR. MacCARTHY: Thanks. I want to talk to you a little bit today about some of Visa's security and anti-fraud programs, and especially as they relate to the Internet. As most of you probably know, Visa is the leading provider of payment services on the Internet. Payment cards account for about 95 percent of the payment services on the Internet and

Visa's got over 50 percent of that share.

So, you know, for us, it's an important part of an emerging channel of commerce. About 2 percent of our volume today is Internet-related. We expect that to grow pretty dramatically over the next couple of years. But there are barriers to electronic commerce.

I think some of you heard yesterday some of the discussion about people's reluctance to shop online. Some of the surveys that we've got indicate that credit card security is the leading barrier to online purchasing for e-consumers. In one survey, 79 percent of the people suggested that credit card security was a problem for them, ahead of privacy issues involving personal information, ahead of concerns about not being able to see or feel the merchandise, ahead of concerns about shipping or handling charges.

And in other surveys, consumers have said that of the features that would be important to them to get them over the barrier to entry, credit card security is listed as number one by over 60 percent of the people. So, for us, security on the Internet is an important issue.

We've tried to address that through a number of issues, one of which, a couple of years ago, we instituted a zero liability policy. As most of you probably know, Federal regulations limit the amount of exposure for credit card fraud to $50. We reduced that on our own to zero so that the

customers should feel confident that if there is fraudulent use of their card, either on the Internet or off the Internet, they're fully protected by that policy.

But we wanted to go beyond that as well, and let me just list some of the other programs that we've got in this area. We've got a cardholder risk identification service, which basically helps identify fraudulent transaction patterns and it stops the merchants from accepting a fraudulent transaction at the point of purchase. We've got an issuance clearinghouse service, which protects consumers and issuers from fraudulent applications and account takeovers. It's very important from the point of view of identity theft.

We've got address verification services. If the merchant is uncertain about the identity of the person, they can ask the address and it helps to ensure the merchant that the person on the other line -- on the line or on the Internet is the real cardholder.

But I want to focus on three of our programs today. One is an education program. We have an Internet shopping guide for Internet consumers. We have a cardholder information security program. And lastly, we've got a new program called Verified by Visa, which was mentioned at the discussion yesterday.

The Internet shopping guide is found on the Visa

Web site. It's pretty basic stuff for Internet consumers. Shop with merchants you know. Look for signs of security. Don't send payment by email. Shop with reputable merchant sites and so on.

We think it's that kind of basic information about security and privacy practices that will help consumers take precautions on their own.

But an additional program we've started up is our cardholder information security program. It started a couple of years ago, as we became more and more concerned about the reports of intrusion into databases on the Internet.

And so, to address consumer concerns about unauthorized access to these merchant databases, we developed new security requirements for cardholder data. The requirements apply to any entity that holds Visa card data, including web merchants, gateways, Internet service providers, as well as the Internet merchants themselves. And these requirements prescribe how companies should store, encrypt and limit access to cardholder data. For example, they require the Internet merchants to install firewalls, to keep security systems up-to-date, to encrypt stored data and to use anti-virus software. These became effective in May of 2001, so about a year ago.

We offer assistance to Internet merchants that accept Visa cards to meet these requirements. We provide

merchants with training sessions, interactive reviews, compliance and monitoring consultation, and information on third party firms that are specializing in consultation and testing.

Under this program, the top 100 e-commerce merchants, who account for about 70 percent of Internet commerce in the Visa system, they are required to have their online security systems validated by an outside accounting or Internet security firm. Other online retailers will be subject to more random security reviews by Visa. There's a lot more information about this program, including the 12 security requirements, on the Visa Web site, and a lot of explanatory detail for web merchants to explain how they should take some steps to come into compliance with the program.

The Verified by Visa Program is a new program we've put into place. It's designed to -- it's just in the pilot stage, so it's just beginning. It's designed to provide consumers on the Internet with passwords. They go to their issuing bank, they get a password. Then when they go to shop online, there's a pop-up screen, they enter the password, a message is sent to their issuing bank that verifies it's the right person. That message then is sent to the Internet merchant. The merchant, himself, never sees the password, so this is not the kind of thing where merchants

can gain the password by looking at the information that comes from the consumer.

We think it will improve security for all parties concerned. I think yesterday many of you might have heard stories about how many consumers are willing to enter PIN numbers if it would increase their security. We found, in our surveys, that 70 percent of consumers indicated that they would feel safer in transactions if they had a PIN number that would improve the security of the transaction.

So, in summary, we've got our zero liability program, we've got an education program, we've got the cardholder information security program and we've got Verified by Visa, all attempting to address the issues of information security. For us, it's good business. We're only part of the effort involved in promoting Internet security, but we think we're an important part of that effort.

MS. FINN: Thank you very much. Next we are going to hear from Fran Meier. She's the Executive Director of TRUSTe, which, as most of you I'm sure know, is a non-profit organization that is known for its Internet privacy seal.

MS. MEIER: Thank you, Ellen, and thank you everybody here at the FTC for having us.

Yesterday I was flying back from the Bay Area and it reminded me of a story. The pilot -- there's a full

plane, it's nighttime. The pilot comes up and says to the passengers that, you know, bad news, radio communication's down, electrical's not working real well, the navigation system doesn't work, and basically, you know, when he gets right down to it, they don't quite know where they're going. They don't know where they are. But he says, the good news is we're making very good time.

I think what this shows is that you really have to have a plan. It doesn't matter how fast you're going. And that is one of the things that we try and counsel our licensee members of 2000 or so that we have. We definitely look at security through the lens of privacy. That is our job. We deal with these issues every day and try and help our licensee members.

Basically, we all know, quite honestly, while there's tension between security and privacy, you really cannot have privacy without security. We also know that security is not just technology, and so, we really try and counsel our companies, and these range from the very small to the very large, about the other aspects of security that they could bring to bear, even if they don't have unlimited technology resources.

Our program requires that companies take reasonable security measures and they have to attest to that. Right now, we have not given very detailed guidelines because

of some of the barriers in terms of the different sizes and the different resources. But we think that there's a number of things that we can help them to do.

First of all, let's have a realization that you really can't have privacy without security. There's more data than ever that is being cut, pasted, synthesized, organized and accounted for. There's really a lack of understanding and a lack of knowledge about what is sensitive data. I'm sure we could even ask people in this room and we'd come up with different definitions of what is sensitive data. But for any given organization, they might know exactly what they're talking about or they may not.

There's more requests from large organizations, from internal functions, as well as external companies, to share data, and it's surprising to me how many companies don't even know where all those data flows in and out occur.

Information leaks arise. We call these data Valdezes. From mistakes to overly broad access to data or sometimes just lack of education about knowing how to use a BCC line. I sometimes forget that.

So, what we have found is it's not just a technology problem. There's many different elements, and the four ones that I'm going to talk about today are, first, education; second, policies, procedures and processes; third, technology; and fourth, and not entirely self-serving, I

think the world of third party oversight is extremely important.

In terms of education, we think that this is probably the most important step a company can take. Most of this is around employee training and management education. We've come up with a poster that we think, in a very basic way, outlines the fair information practices and it's something that should be put in a data processing room.

But in terms of training employees, our guidelines are this, regularly training your employees on the privacy issues. Make them read your privacy statement. Make them understand the privacy statement. As far as the employee orientation, give them the privacy statement and emphasize that this is an important value of the organization and something that they're going to be measured on and monitored.

In addition, make sure they know when to escalate privacy issues. When they get into situations where they don't understand what to do, what the actions are, maybe they're facing some technology they don't know, give them some guidelines so that they can escalate the issues.

Document problems across organization. Try and have some sort of internal monitoring. Put in place some measurements. So, you know, the idea is, if you can't measure it, then you really can't monitor it and you certainly can't manage it. So, you need to address those

things.

Try to have some systems that can measure and monitor, and finally, try and find a way of monitoring and auditing what you've done. So, maybe it's a different outside group externally or a different group within your organization that could come in and oversee from a different perspective the privacy programs.

Again, education is extremely important. Along with that comes a lot of policies and procedures. Let me talk to you about some of the key questions. Who has access to what data? When is access reviewed? Who can revoke access? What are policies around providing or revoking access? Access is a very important part of understanding security.

I mentioned this earlier, sensitive information. What is your policy? Who has access? What procedures do you have that are different sensitive information versus other kinds of information?

Email, we all know about the email problems. We're not just talking about SPAM, but about copying the world and disclosing potentially personal, harmful or sensitive information. Make sure there are processes.

Passwords, this is not only for your internal employees, but for your customers. How often are they changed, how are they encrypted, how are they stored, when do

they change, et cetera?

Authentication, very much related to passwords. What is your data retention policy and how often do you change that? And, again, who gets to make the decisions?

We had a little earthquake last week in the Bay Area. It reminded us about natural disasters, what's your back-up plan? It was a very small earthquake.

Third party sharing. You know, what are your procedures in place? Again, access. And with your third parties, what kind of NDAs do you have, how are they enforced and are they audited? With your partners, the same kind of thing.

Audit trails, will you be able to be audited? Do you know where things are going that somebody could come in and do an audit? Do you have an audit trail?

And then, finally, if disaster happens and something leaks and you have a problem, what are your procedures after that?

So, again, when you think about education and policy and procedures, none of these things necessarily talk to technology. But technology is the next important point. It's ever-changing. Companies need to create a strategy for technology. They need to know where they're going. They can't just be buying equipment without having the other things in place, however, or else it's really garbage in and

garbage out.

This does not mean finding the most expensive firewall or the most -- the largest, you know, technology staff. But I think there's some simple things that companies should -- even small companies should do. They should try and look at their company from a hacker's point of view. They might want to consider having a vulnerability scan. That allows companies to be proactive about security. They might want to create some way of keeping themselves updated.

And, finally, I'd like to talk to oversight. I think TRUSTe performs a really good role with our member licensing network to give them another set of eyes, to look at what they're doing in terms of their policies and procedures, to make them attest that they have reasonable security, so at least internally they ask the question, do we have reasonable security. And, of course, I think we provide consumers with a trusted dispute resolution program to help them identify and resolve, and sometimes for the company, provide the first red flag that something's amiss.

And for the businesses, I think it's -- we demonstrate and help them demonstrate to consumers and to the government alike that they are meeting reasonable standards. And, of course, I think that we help them with compliance.

So, again, the solutions that we recommend to our licensing members are education. To that end, we are also

working on a program to develop education for employees with one of our partners, ePrivacy Group. I think in terms of policies and procedures, we're defining more and more. Third, in terms of security, we are looking at introducing to our member licensees different solutions, different technologies, certainly not prescribing anything, but there's some good things out there that I think make sense, such as Lucent Security does vulnerability scans that we're interested in.

And then, of course, we think partnering with TRUSTe to bring TRUSTe to your network of licensees or to introduce more companies to third party oversight really makes a lot of sense. Thanks very much.

MS. FINN: Thank you, Fran. And last, but definitely not least, is Larry Ponemon, who is the Chief Executive Officer of Privacy Council.

DR. PONEMON: The best part of being the last person is I just get to say ditto, ditto, ditto, ditto and ditto. There's really nothing new to add.

But actually, I'm Larry Ponemon and I'm the CEO of Privacy Council. We are a privacy and data protection firm headquartered in Dallas, Texas and we have offices here in D.C. and in Philadelphia. We provide knowledge products, automated solutions and advisory services to business organizations on a local basis, and we have a division called

Net Diligence, which provides security and cyber risk assessments, and it's often used as a precursor to receiving a cyber insurance policy or insurance coverage.

And so, what I'd like to focus my conversation on this morning is how cyber risk insurance, the industry itself, could actually help to shape better corporate security practices and perhaps even standards. So, that's going to be the next five minutes, and then I'll stop being a talking head, I promise.

First, if you know me, I always have a story, and this is a story that probably goes back about now almost three years ago when I was a partner at Price, Waterhouse, Coopers. As a partner in PWC, you do audits, and we did an audit, a privacy and security audit of a major financial service company, and it was really a well-done audit and it was against standards that we and the client developed together. These were really great standards. And the goal of the audit was to make a presentation to the audit committee to show that this company was a leading edge company with respect to information security and privacy practices.

So, we did the audit and we found out pretty quickly into the process that most of the stated practices and standards were not being complied with. One example, they implemented an intrusion detection system, state-of-the-

art IDS, and they basically identified over 40,000 intrusions to their system every week, which was a big number. And, in fact, the CIO was proud of the fact that their technology identified such a large number.

(Laughter.)

DR. PONEMON: However, the chief information security officer who reported to the CIO said, I don't know what to do, I'm at complete information overload. Probably about two of the 40,000 were really serious intrusions. The other 39,998 were probably like hackers, like my son, David.

MS. MEIER: That's not serious?

DR. PONEMON: I'm just joking. No, that's very serious. I'm just joking about my son doing that, maybe not.

Now, what I'd like to do is talk a little bit about the analogy between insurance in kind of the physical world versus the cyber world, and we think about insurance -- you know, you get a policy, a homeowner's policy and if you have a fire alarm or you have locks on your doors, smoke detectors, and all of that good stuff, you actually get an insurance reduction. And similarly, in the cyber world, if you have things like firewalls and filters, you have seals, you have intrusion detection software, anti-virus software, strong form authentication and so forth, there's probably a good argument for premium reduction.

And if you kind of think about the recent

introduction of insurance, cyber risk insurance, the general view is that even with insurance, there is no fail-safe system. There's no such thing as 100 percent protection. So, even if you use the best technology, even if you have the greatest standards, even if you have the best auditing firm in the world, it's still not 100 percent. There's no way there could ever be a technology or standard or auditing solution that is 100 percent effective at mitigating risk.

So, possibly insurance is the best means to address that residual risk, that little risk that is always out there. And if you kind of look at the scene for cyber risk insurance, it's still a relatively new and very young field. I think it started about 1998, maybe 1999, and cyber risk policies usually include such things as privacy and trademark and copyright infringement, maybe even defamation, libel and every slander issue.

Following the brick and mortar example, the analogy I discussed before, companies that seek to implement the best possible data protection practices to qualify for cyber insurance protection, that's probably a good thing. If you think about the short term carrot, the really big carrot now for companies right now is that if you do all of the above correctly, you can probably buy the insurance at a lower premium. And perhaps if you tie it with a verification process, there's probably a longer term confidence because it

may create additional comfort and even credibility and trust.

So, right now, if you kind of think about the development of the insurance industry, insurance today is about protecting risk. Insurance tomorrow can become a signal of credibility.

How big is it? How big is the problem? You know, if you look at some of the stats about how large that residual risk is, on the low end, the most conservative estimate, based on incomplete data, is about $11 billion. Other estimates go as high as about $45 billion even today. And there's really increasing risk in cyber risk insurance.

And really, the major focus of a lot of companies is on insuring against virus attacks, denial of service attacks, hacking, Web site defacement and even the employee misuse of email. So, we really think that as this industry develops, insurers could actually become a major, major force in shaping just reasonable standards, standards that could be complied to by most organizations and this, by the way, is not new stuff. Insurance has shaped standards in the construction industry, for example, and the auto industry.

Now, how large is the industry today? The insurance industry, a couple of years ago was zero. Now it's at about $100 million. Well, that may not seem like a large number. It's positive infinity growth, so that's not bad. But it's projected, according to a Business Week article, to

be a multi-billion dollar industry.

Now, my last part of my conversation this morning is -- what I'd like to do is just discuss post September 11th, and we basically consider that there's a balancing act that needs to happen between privacy and security. And we basically think that we have to trade off one for the other. And I believe that security, like Fran mentioned earlier, is a component, a vital component of privacy. And so, unless your information and information security infrastructure is secure, privacy is at risk. In other words, a sound privacy policy is completely worthless without sound risk management policies.

I just want to talk about my top 10 list, but I'm going to reduce it to five. Our Net Diligence Division has identified 10 tips for managing cyber risk, and if you're interested, if you want to sleep tonight, this is a good thing to read before you go to bed because it has a top 10 list. You should read that.

And really, the top five of the top 10 starts with, review your policies and make sure they're real, make sure that you can actually do what you say. You could be walking the talk. And you need to conduct an e-risk assessment. Conducting an e-risk assessment shouldn't be that difficult and it doesn't have to be at the level of detail where you have to know where every specific piece of

information resides. But a high level assessment that is across the board that has good coverage is very, very important.

It is also important to establish baseline network controls. You need to develop a response plan, and Fran mentioned that, I think. It's just a matter of time before you have the security Valdez. And then, consider insurance to address your residual risk.

Just the last, last point, I promise. We are starting to collect incident data because we think that one of the problems for the insurance industry is the ability to underwrite risk. So, if you talk to underwriters, they are really concerned that if they give you a policy, that there could be some gigantic catastrophe and they want to make sure that they can get a handle on that before they provide the big policy.

So, we're working with the insurance industry to really collect real incident data, and this is going to help shape the way premiums are written and hopefully this could create greater demand on the insurance industry for this type of product.

So, without further ado, I think it's time for questions. Thank you.

MS. FINN: Thank you very much. Let me start with a broad question that maybe all of you can address. There

are a lot of different standards that you've talked about, a lot of different ways the standards are emerging, and you didn't even touch on some of the ones that were mentioned yesterday in terms of the Gramm-Leach-Bliley safeguard standards, the FTC's rule just became final last week, HIPAA which includes security things.

How do the various standards differ or work together and how will they play off of each other if at all? Do any of you have thoughts on that? Mark?

MR. MacCARTHY: Yeah. I can't speak to all of them, but the -- just to comment on the FTC standards and the ones that were also put in place by the banking regulators. They are basically process standards. They say, you know, you have to do the following sorts of things in terms of having a policy, having a person responsible and so on and so forth. They were not what people have been talking about before, technology forcing or mandating standards.

So, they took the right direction, which is to focus people's attention on doing something in the area of information security, but not sort of tying it down so that it couldn't change or develop in the future.

Our standards -- we've got 12 of them, we call them the digital dozen -- they're out on the table outside for those of you who want to look at them and review them. We took a couple of years to develop those standards and we

did it by looking at what was out there, talking to information security companies. We know a lot about security ourselves, and after talking to our big merchants and seeing what they felt comfortable with, we worked fairly closely in putting them in place. As I said, they've been in place for about a year.

There are other standards in the same space and for those companies, it satisfied the other standards. We have a provision in place that a review, for example, of internal processes is being conducted to satisfy another set of standards, can also be used to satisfy our standards. We've got to do our standards as well. But the process of having an external review, we don't say you've got to have two separate reviews. So, there are certain efficiencies that you can become involved in that will allow people to live with multiple standards that need not be conflicting.

MS. MEIER: One of the things I'd like to emphasize is that for consumers, for them to feel like there's standards of security, it's really helpful to have something that shows them. So, I think the seal programs, I think the Verified by Visa Program, anything consumer facing can have a lot of impact if it's a company with some education or if it has some brand-powering in and of itself. So, we're really looking to try to incorporate the best practices into our seal program because we know that

consumers really recognize the seal to stand for privacy especially, and I think it's a very powerful way of getting that across to consumers.

And, you know, consumers don't want to know about firewalls and hackers and the details. I mean, quite honestly, they just want to know things are okay, and we need to do a better job of making sure things are okay and communicating that to them.

MS. LIPPS: I would just add in the BITS criteria, we do look at what regulation is out there and then we map that regulation to the criteria that we're developing. I would say that they work really well together, back to Mark's point of the regulations being sort of at a policy level and then us drilling down a layer, here are the considerations. If you have to have an access control policy being the regulation, and then we would specifically say, these are the access control elements that need to be considered.

DR. PONEMON: I think the issue -- I mean, these are all great ideas, but I think what may be missing are hammers and carrots. On the hammers side, you basically need to come down pretty hard on organizations that don't comply.

In my little example, one of the -- the story I told before, one of the issues that occurred when we finally reported to senior management about how bad they were -- how bad this organization was with respect to practices, actual

practices, they wanted to reduce the standards. They said, well, the standards are just too tough. So, if we reduce the standards, can we actually get a clean audit opinion?

(Laughter.)

DR. PONEMON: We thought about it. Actually, no, we didn't. But the reality of that is the hammer. You need to have some reasons why organizations have to comply. Maybe it's loss of insurance, maybe it's just embarrassment, maybe it's just in some report to the Federal Trade Commission. Without that hammer, unfortunately, in light of these great ideas, it may not work. It may not be practical.

MR. MacCARTHY: Can I just jump in there?

MS. FINN: Um-hum.

MR. MacCARTHY: I mean, maybe I wasn't clear, but the hammer in the case of the Visa rules are that if you don't comply after a reasonable period of time and discussions with us, we begin to fine you and we increase the fines, and ultimately, if you don't provide the kind of security we think is important for consumers to have on the Internet, you can't use a Visa card.

MS. FINN: Mark, I wonder -- following up on that, and Kimberly, I'll let you jump in. But what has the experience been with the standards? You said Visa standards became enforceable in May of 2001. Have you had time to sort of do a first round of trainings and compliance monitoring

and things like that? What has your response been from the merchants?

MR. MacCARTHY: The merchants are largely supportive. I mean, we've had about a year. We haven't had a company, as of yet, that said, no, we're not going to do it. We're in discussions with all of the top 100, at this point, and we're beginning to look at the second tier, the second 100.

The response has been largely positive. I wouldn't say it's been uniformly 100 percent, but it's been largely very, very positive. Merchants recognize that this is something that ultimately is in their interest. If something really does go wrong, it can be a life-threatening situation for an Internet company. And so, they're prepared to work with us and be comfortable with the kind of reviews that we're requiring and the kind of internal processes that we're requiring.

MS. FINN: Kimberly?

MS. KIEFER: I was just going to add that we -- in looking at the hammer from the liability side, for those organizations that aren't subject to the specific standards, such as HIPAA or Gramm-Leach-Bliley, we often refer them to review those standards and guidelines as more applicable industry wide, especially in light of the Eli Lilly case from the FTC, which brought quite a few -- most of the content of

the now finalized rules over to a company that wasn't regulated specifically by Gramm-Leach-Bliley.

MS. FINN: I think, at this point, I will also open up the floor for questions from the audience, and if anybody's listening in the overflow rooms and they would like to ask a question, you can come up to 432 here. There's a microphone by the door.

I don't know if you're just standing by the door or if you have a question.

MR. COBB: I was actually going to ask a question.

MS. FINN: Okay. Then I will go ahead and recognize you. Please give your name for the reporter.

MR. COBB: Steven Cobb from ePrivacy Group. I was here yesterday, as well, and I see certain themes emerging, one of which seems to be certification, that organizations seem to want to be able to show to the world, to their business partners, their customers and possibly regulators, that they comply with these standards that we've been talking about. And possibly, Kimberly, you could perhaps talk to what role certification might play in offsetting liability or defense against liability.

I mean, I'm very pleased to see people are finally working on this liability thing. As you mentioned, Eli Lilly has kind of helped highlight that. But it's clearly hanging in terms of security breaches. So, would some form of

certification play a useful role there, if people were certified to some security standard for their organization?

And then, perhaps, Fran, if you could speak a little to the safe harbor aspect of compliance with a program like TRUSTe with respect to regulation. I believe TRUSTe offers that with respect to COPPA and other things.

MS. KIEFER: Compliance with industry standard guidelines, rules, regulations, best practices are a very strong indication and way of minimizing potential liability, and certification would certainly factor into that if it was industry wide reviewed, set forth, for instance, by the Center for Internet Security or a group like that. However, case law is very clear that complying with some sort of guideline, industry standard guideline, does not immunize you from liability.

But at this point in the development of security and trying to minimize your potential liability, any sort of certification, you know, we're still at the first step. Any sort of implementation of security measures is better than nothing and is what most companies need to do at this point. Just -- even two measures, such as a comprehensive security program and good monitoring, training and awareness is going to do a lot to minimize potential liability at this point.

MS. FINN: And then, Fran, do you want to pick up the other question?

MS. MEIER: Yeah, just to pick up on that, I think that the process of going through certification often is the thing that is going to protect you and help you with liability, because if you have to go through a detailed process, you're going to have to look at yourself, look at your procedures and step up to it.

I think we offer safe harbor for the Children's Online Privacy Protection Act and for the EU. We think that these make sense. Safe harbor at least gives the companies some guidelines that are transparent to them, that we can help them through. It gives them a certain amount of protection -- well, a good amount of protection and liability, and I think the safe harbor concept is better to keep up with the changing technology and the changing business requirements better than legislation at times. So, obviously, we're big proponents of safe harbor.

MS. FINN: Okay, next question?

MR. LLOYD: Hi, my name is Rich Lloyd. I run our CRM practice at Dell Computer. My question -- kind of a statement and a question. My company has a real belief that standards adoption drives value and economic value to consumers. And I believe that that principle applies in the realm of privacy, certainly, as well. But what is difficult, I think, for a business leader, such as myself, and for corporations right now is the question of where to put our

energy around standards.

The civil, public and private community feels very diffuse in terms of what are the standards and where those standards should be driven and how those standards should be driven. And for well-meaning companies, such as ours, that want to continue to be very involved in privacy and privacy matters and protect our consumers' best interests, it feels difficult to know where to direct our energy.

And I was wondering if the panel members could comment on that.

MS. FINN: Larry?

DR. PONEMON: That's actually a great point. The problem is that everyone believes, or not everyone, but organizations that set standards believe that their standards are better than the other guy's standards. And if you really look at standards, whether they're for privacy or information security, probably about 80 percent or 85 percent are really grounded on the same basic principles.

So, I think what we really -- I mean, I hate to use the accounting industry analogy. Unfortunately, I'm not sure if it works anymore, but for a time it worked and it worked really well. And what you had was a group called the Financial Accounting Standards Board that represented industry, different constituencies, and they got together and they studied complex issues and created standards, and these

standards, for the most part, were sensitive. It wasn't like one size that fits all, but it was also a set of standards that was universal, that applied to all organizations.

So, I think we need to do some of that, otherwise we have this diffuse issue that you're talking about where, you know, whose policy prevails, what policies are the best policies. That's just my view.

MS. MEIER: On the contrary, I think you should have seals that show consumers that you take their privacy and security seriously, and whatever seal you think does that best would be the thing to do.

MS. LIPPS: It sounded to me like implied in your question was a concern about, you know, investing a lot into standards areas where there may not be a significant return, you know, on that investment. And, you know, I think if you try to develop programs that are comprehensive, but are universally applied across the entire organization, sometimes that can be challenging and I think not necessarily of benefit to an organization.

I think that in -- at least the members that I've worked with, tend to look at the critical services that they're delivering and prioritize those, and they have to ensure that those services are delivered reliably to their customers. And so, that helps to somewhat shape where you put your energies and your investments.

MS. FINN: Kimberly?

MS. KIEFER: One last comment. I think the difficulty that you're running into stems as well from the different types of standards and what area -- and I hate to use the word "granularity" but what level of detail -- what types of standards addressing what part of information security.

Are you looking at standards for enterprise security that may be focused or targeted at an information security program, or are you looking at standards for software development and operational benchmarks, which was mentioned yesterday. The Center for Internet Security is working on those type of operational benchmarks. Or are you looking at products security, types of standards, such as common criteria that are targeted at products, at certifying products or systems?

Another one is standards for the system security. And then, finally, do you want to stay at the top level where it's more best practices and guidelines and recommendations?

MS. FINN: Is there anyone else waiting to ask a question?

MS. CARLSON: Arlene Carlson with eWeek again. How do any of the five of you use the OECD guidelines and do any of you anticipate that the revised guidelines will have any impact on the standards and guidelines that you advocate?

Is anyone waiting with bated breath to find out what the revisions are?

MS. KIEFER: If I could address that, yes. The OECD security guidelines are very important for setting the principles, the commonly accepted security principles from which best practices can be derived. So, the old version and the new version, not waiting for them, but just that we're having some -- you know, that we have consensus and we have these commonly accepted security principles are extremely important to work down from.

MR. MacCARTHY: We're looking forward to them because I think they will, along with lots of other things that are going on in the industry, they will help to focus the attention of the business community and others on the importance of information security. I think the details -- you know, we haven't seen them, so how to use them in practice is not clear to us. But clearly, they are being well-developed. The process looks pretty good to us.

And so, we think that those principles will be very helpful in spreading the good word about the importance and the need for taking steps in the area of information security.

MS. MEIER: I would just agree.

MS. FINN: Anybody else?

MS. MEIER: The only thing I would add is just

that we're looking forward to the blending, I guess, of a lot of different principles, ultimately. Perhaps the OECD can be the umbrella for a number of activities that are already underway, the Basel Committee's work, the E-Banking Supervision Group under Basel that has developed principles in that area. So, if there is this umbrella set of principles under which all of these other initiatives, international cyber security principles, et cetera, can fall, you know, we think that would be a very good thing.

MS. FINN: Okay. Is there anyone else who would like to ask a question or make a comment?

(No response.)

MS. FINN: Okay. Well, I think we have just a little more time, so let me ask another question. Most of the standards that we have been talking about are standards that are directed towards businesses.

But in talking about seals and whether or not there is some kind of seal that you could have where consumers would know it's secure, you don't have to know if I have a firewall or an IDS, you don't have to know the nuts and bolts, but you can look at this and take some comfort, do consumers understand even what that seal would mean, how much comfort to take from it, and could there be some way to have different levels of sort of security certification that would mean something to consumers or is this an area that is

inherently so complex that that may be difficult to arrive at, something that would allow consumers, in some ways, to make choices about the level of security they want versus other features?

Mark?

MR. MacCARTHY: We like seals. I mean, Visa's working very closely with BBB online and their reliability program. We think it's the kind of program that -- when merchants participate in it and display that seal, it's a good indicator to consumers that this is a reliable merchant and you can trust that merchant to engage in good consumer practices.

There's nothing quite like that yet in the area of security. We thought about a separate security seal for the people who comply with the new Visa cardholder information security program and we decided against it. Ultimately, you know, we're hoping that the Visa sign itself will come to stand for good security and that people will see that flag and say, okay, I can work here because these guys are engaged in good security practices.

But yesterday, there was some discussion -- I think Dick Clarke mentioned that consumers need to know more about what's going on with the security practices of the Web sites that they visit, and I think some of his suggestions were very, very positive.

We are thinking about -- we haven't done this yet -- maybe a requirement on the merchants not only to comply with the Visa program but to say that they're complying with it. That way, you know, consumers would be able to read as part of the disclosures that are on the Web site that they comply with a tough security program provided by Visa. That may be helpful to them.

But as far as I know, right now, there's no unique seal that would guide consumers and tell them that shopping here is okay because the cardholder information that they've got will continue to be kept safe.

MS. FINN: Larry?

DR. PONEMON: Yeah. The -- I'm a big supporter of seals. I think it's a great idea. The problem is a security seal is also a bullseye. So, for example, if you're a -- you know, again, a hacking community, these evil folks out there that really love to penetrate systems that probably have the seal will be more likely to be the target of attack, that's a problem.

I think the second issue is a seal -- it goes back to the issue -- is a meaningless thing unless you have standards and unless you have ways of verifying that an organization is walking the walk. And so, a seal that basically says it's here on our Web site until consumers start to complain is not really going to add much value. In

fact, it will probably destroy the potential to really create valuable verification.

MS. FINN: Fran, did you want to comment?

MS. MEIER: Yes, please. I think that we have found that we're very fortunate to have been born in the early days of the Internet, that people widely recognize the TRUSTe seal. And while we know about respect for personal information and privacy, we also know that security is a big part of privacy, and consumers kind of equate identity theft, security, privacy, all in one.

So, I think by having that very prominent seal out there, having companies go through a program and meet the appropriate requirements and get certified as to those privacy requirements really makes the seal powerful. We know that people will change their behaviors and trust an organization more if there's a seal there. We know that we are the most widely recognized seal and we know that people are looking for the seals to stand for something. We all need to do a better job of educating consumers about what the seal does and does not mean.

Over the years we feel it is more than just say what you do, do what you say, although that's a very important part of it. But there are a number of, I think, standards that we have to look up to and that will be increasingly part of our evolution.

MS. FINN: Just one last check on questions from the audience and then we'll have a short break.

MS. BRADY: Hi, I'm Nancy Brady (phonetic) from Price Waterhouse Coopers. I'm just wondering regarding this seal for verification. I do know there was a recent survey sponsored by various accounting firms and they did actually come up with that consumers are looking for a seal, that sort of thing. I expect in a few years we'll probably see some certification by some of the accounting firms as well.

My question actually regards Visa. What I was wondering is, I know you have this cardholder information security program and that program is geared towards online merchants, which I think you said maybe accounts for 2 percent of your payment services today. So, what about the other 98 percent?

I personally was subject to fraud. My credit card number was stolen. I believe it was probably somebody who actually worked at the merchant. What programs are you going to try to do as far as the mom and pop shops? Do they have to have more security? Do their receipts have to provide -- you know, X out half of the numbers, that sort of thing? Do they need to have their consumer data also encrypted?

MR. MacCARTHY: In general, the merchants have always lived under a generalized requirement to keep the cardholder information secure. That's been a requirement for

our merchants. And we took special steps in the area of the Internet because of the intense publicity about intrusions on the Internet and because Internet merchants tend to keep their cardholder information in a fashion that they're more exposed to intrusion from an open network, whereas the offline merchants keep their data in a much more secure situation.

But they all live under the generalized requirement to exercise appropriate caution to keep the information from being available to unauthorized people. In terms of the generalized fraud stuff, we think we've done a pretty good job on fraud over the years. In the late eighties, the fraud rate was 20 cents for every $100. In the early nineties, it dropped to about 15 cents for every $100. Now, it's down to seven or eight cents for every $100, and that's a result of the programs that I described earlier in my talk.

The fundamental thing that protects consumers is the zero liability policy. If your card is compromised and someone gets it and uses it in an unauthorized fashion, you are not liable for the resulting loss.

We talked about the checks and a lot of the merchants are now using the electronic devices that X out the last five digits. In five states, it's required to do that. There's a bill pending in the Senate Judiciary Committee that

would make it national policy. That would be a good result and we think that would be helpful to everyone. That would mean you don't have to tear up all those receipts anymore because it would be done for you.

So, I think we've done a pretty good job of focusing our current efforts on the Internet where the problem is perceived to be great. But we have to start using the other efforts that we have to keep fraud at a minimum.

MS. BRADY: I think the only thing I would add to that, for these guidelines that you do have for the Internet, that maybe you can also share them with your other ones because a lot of these people are using computers now, although they're not networked, but they have broadband access, customer databases, everybody's address. Because those are definitely very good guidelines.

MR. MacCARTHY: It's going to be one step at a time. In fact, many of the people who are online, and offline merchants as well, to the extent they have merged databases, which many of them do, the guidelines would, in effect, provide protection for all the information that they've got.

MS. FINN: Thank you. I'm going to stop the discussion at this point so that we can take a quick break. We'll resume at 11:30 with our next panel. Thank you very much for coming.

(Applause.)

(End of Panel VI discussion.)

PANEL VII: ALTERNATIVE APPROACHES

MR. EICHORN: We've got a full house for our last panel of the workshop. Before we get started, I just have a couple of quick announcements. One is that at the conclusion of this panel, Commissioner Swindle will be making some closing remarks to tie up the workshop and also if -- some of you may not have noticed, there are materials outside on the table where the folders are available. Some of the speakers that made presentations made other materials available. So, you're welcome to partake in that.

This panel, we've titled it Alternative Approaches, but it's sort of a panel of, you know, what's the future, and we're going to be looking at the future in a whole different variety of ways. Some people have interesting ideas or business models that they're going to be implementing and some people have ideas about who could do what or who should be doing what. And, you know, as far as the business models that we've discussed over the course of the workshop -- some of the companies that we've had represented in other panels could equally well have been represented here. So, there's a lot of good, imaginative

ideas and security tools out there.

Without further ado, I'll proceed, starting with Paul Collier on my left. Paul serves as Executive Director of the Biometrics Foundation and he's a founder of the consulting firm ID Technology Partners, Inc. and a founding member of the International Biometrics Industry Association. Paul?

MR. COLLIER: Thank you, Mark. Just a little history, the Biometrics Foundation is the 501C(3) non-profit foundation in the biometrics industry space. Our charter is primarily research, education and standards. We're partnered with the Center for Identification Technology Research at West Virginia University, which is the National Science Foundation designated center for biometrics.

We were chartered by the International Biometrics Industry Association about two years ago. IBIA was formed in 1998 as a true 501C(6) trade association. The very first thing IBIA did was embark on a program of education and setting standards and codes of ethics for the implementation, development and deployment of biometrics.

For those of you that have heard a lot about biometrics since September 11th, especially, there are some misconceptions in the marketplace about what biometrics are and what they bring to the party. It's a good thing for Hollywood, you know, with iris scanning and fingerprint

recognition and voice recognition, et cetera. But these technologies have matured and are now in the marketplace and are reaching critical mass with regard to their employment in various market applications.

What biometrics bring to the party is a piece of a positive user authentication model. They are not a panacea, they are not a silver bullet. But when used in concert with other technologies, they can significantly raise the bar with regard to positive identification.

With the Internet, we are faced with unique problems that we've never encountered before. Back in the seventies, I remember reading a book called, The Wired Society, where it predicted exactly what's happening now. There's less and less human interaction. There's less and less human safeguards as we go about our day-to-day lives. And especially with regard to the transfer of money, you don't interact with a teller at the bank anymore, you work through either PC banking or an ATM.

So, as we remove these human safeguards, we have increased the possibility of fraud and theft, especially with regard to our identities.

Back in the mid-eighties, the Federal Government embarked on a program of research and biometrics. Actually, it was championed by the National Security Agency because they also had the need to see actually not just

authenticating hardware through a network, but authenticating a user to an enterprise system or network. So, they embarked on this program where they would work toward developing a stronger positive authentication model.

What came out of that was the something you are, something you know, something you have model. Something you are is the critical piece that's been missing for some time. Because I can give you my token if the token's required to log on to a network. I can give you my password or my PIN, but I can't give you my fingerprint or my iris or my face for you to log on. So, it really is the final piece of something that, if implemented, can ensure that we know that it's you sitting in front of the monitor.

Secure transactions over the Internet have been an issue. I think e-commerce has been held back because of a perception on the part of the consumer that their credit card is going to go out over the Internet and someone is going to steal the number. They are not reluctant to give it to a waiter in a restaurant that can take it back in the kitchen. They're not reluctant to give it to someone over the telephone who calls them to sell them concert tickets, but the idea of putting it out over the Internet has always been an issue.

Without proper audit trails and without proper user authentication, I feel that the consumer will still show

a great deal of reluctance to use the Internet in an e-commerce mode.

Identity theft has got to be one of the most horrific crimes that's been perpetrated in the last decade or so. Other crimes against property and persons are one thing, but the amount of time to recover from identity theft, if you can at all, to repair your credit and replace the money, et cetera, is significant.

I know we've all heard some horrific stories about people whose identity has been taken, misused. Their bank accounts have been emptied, their credit has been ruined.

Biometrics has also gotten a lot of bad press because there's still a little voodoo under the hood. It is a science designed to identify us by a unique human attribute. I think it's that factor that makes people concerned. It's just that it's not just another technology, but it is just another technology. It's a new technology that has been perfected and ready to move forward into the marketplace. The computer industry embraced it. Bill Gates has used the term biometrics. Actually, Compaq, Microsoft and IBM were all three founding members of the Bio ABI Consortium, which is now an ANSI standard for integration of biometrics technology into computer systems and embedded solutions.

Again, I think it's important that we realize that

they're a part of a bigger mix, a part of a bigger model, and they are, again, the only thing that can give you non-transferrable authentication, whereas the others are transferrable.

MR. EICHORN: Thank you, Paul.

Jeff Fox has already appeared on the first panel. As a reminder, he is a Senior Projects Editor for Consumer Reports Magazine.

MR. FOX: There's been a lot of discussion since yesterday about e-commerce and business security, but I want to sort of bring us back to the other big issue which I talked about yesterday, which is really the problem and the issue that I really researched for my report and that we're very concerned about, which is consumer home security in the home.

So, the bottom line, this story, for those who weren't here yesterday, is in the June issue of Consumer Reports. There will also be information on the FTC Web site based on my research. If anybody wants a copy of the press kit afterwards, I have them.

Just to summarize was that if you had to put a number on this -- our research showed a significant number of consumers experiencing serious economic damage if you take in the aggregate, and I would conservatively estimate that at least $200 million was spent, and possibly in the billions,

by consumers trying to repair the damage from viruses over the past couple of years.

So, just to quantify a little bit that this is an important economic problem.

In terms of some of the ideas of what could be done, first I want to kind of address Commissioner Swindle, remembering your days in the Navy and your question is, would you fly without an altimeter or instrument panel?

I think that, when you're on any kind of mission or any kind of campaign, you need to have good information along the way to know where you're going, how it's going, you know, what kind of progress you're making, and I think -- what I also suggested yesterday -- that we need to have some kind of good regular data from the government that these are crimes. If you want to know how many cars have been stolen or how many people have died in traffic accidents, you can get that information from the government.

But we do not have that kind of information, and if we have a campaign to educate consumers and to make progress and to build this culture of security, the only way we're going to know -- the only type of accountability we're going to have as to whether it's working, whether the problem's getting worse or better, is that regular reliable data from the institution that's primarily responsible, which is the government. In the absence of that data, it's going

to be very difficult.

Another problem that I came across in my investigation from looking at it from a consumer point of view is that most consumers who are victimized by hackers have really no legal recourse. Unless you happen to fit the very specific qualifications of being involved in interstate commerce or maybe involved in an attack on a government computer, the people I spoke with and the laws I checked told me that your local police are not equipped to deal with this. If you go to the state or Federal agencies, in general, they are not frankly terribly interested in the average consumer. And I think that's a problem that needs to be dealt with.

I think that the Federal Government maybe needs to work with the National Association of Attorneys General. You know, maybe it's not something that the Federal Government, by itself, can do. Although maybe it needs to be done in conjunction with the State. But we need some kind of more coordinated system.

And related to that, I would say that there seems to be no locus, at this point, of responsibility in the Federal Government for the security issue. I'm hoping that the FTC will take a lead on this and maybe coordinate agencies. The National Infrastructure Protection Commission really has a bigger job to do and they're not really a consumer protection-oriented agency. So, I hope that the FTC

can take a lead on this.

That leads us into a discussion about public education. We have a National Cyber Security Alliance Campaign that was launched in February. I mentioned yesterday that it was launched when a number of its members stood up and sort of trumpeted their participation in this campaign. I really haven't heard a word about this campaign, nothing on TV, nothing in the newspaper. The weekend when we turned our clocks ahead, which was supposed to be a high point, there was essentially no publicity.

I mentioned yesterday, you know, up in my hotel room there was this little card, you know, with this little dog from the -- my eyes are not as good as they used to be -- the National Crime Prevention Council. This is an example of getting to people where they are. I think that saying we have an online Web site is all well and good, but frankly, a lot of ordinary people, our friends and relatives, don't go -- you know, aren't drawn to Web sites on a daily basis to get that kind of information. I know that -- when I think of my friends

-- whenever I think of this campaign, my friend, Marcy, you know, it's Marcy that I apply it to. Is Marcy going to know about that? Marcy's in her sixties. She's not in kindergarten, she's not a business person. Is it going to reach her? And she's been affected by viruses and viruses.

I'll be watching in October to see if this campaign, you know, when we turn our clocks back again, which will come a little too soon, you know, whether that campaign reaches awareness.

The last thing I want to mention is ISPs and the discussion about making consumers aware when they're getting broadband accounts of whether they have a firewall installed, and there was some discussion about maybe ISPs aren't doing enough. I looked at some ISP -- broadband ISP Web sites. I found not only aren't they doing enough, in some cases, they're actually pretty much discouraging use of firewalls, which is really going in the wrong direction.

The AT&T broadband Web site, for example, says explicitly, AT&T doesn't support, it won't recommend, help install, set up or configure a firewall. That -- I mean, that's not even neutral.

The Roadrunner Web site sits on the fence. They give very emphatic advice about the number of security measures and then kind of this very soft statement about, if you want to do a firewall, maybe you should do one.

On the other hand, I just had an email from CableVision's Optimum Online Service a few days ago, in which they announced a security package that they were offering, including a firewall and anti-virus. I haven't checked up on it yet, but clearly of the three, I mean, that is an example

of the way to do it.

I understand there's speculation as to why they wouldn't say we support firewalls. The answer, to me, is quite simple. It's a support cost. The effort -- you know, the cost of supporting, answering questions, the consultations. I mean, does there have to be a charge for it? I don't know. But I think that we've got to find a way to get our ISPs supporting this. That is the main point of contact for people.

So, those are some of the suggestions that I have.

MR. EICHORN: Great. Peter Harter is next. Peter is Senior Vice President for Business Development at Securify where he manages strategic customer relationships and public affairs activities with governments, industry groups and technical standards bodies. Peter?

MR. HARTER: It's a pleasure to be back here in this room. I've been coming to this room to talk about privacy and security since April of '95. A lot of people wanting to hear about what we call cookies. I'm really happy not to be talking about cookies today.

A little humor. It looks like Officer McGruff, so I guess we should talk to Dick Clarke and see if he can get in a trench coat and make him the Officer McGruff for the Internet, taking a bite out of cyber crime. I'm not going to bark like a dog, but maybe we'll get -- anyway.

(Laughter.)

MR. HARTER: Again, consumers and security -- my company, Securify, started with about 40 people in Mountain View. I guess I didn't get enough of the dot com madness the past seven years of my life, so I'm back for a third time. And we sell our software to banks, the military, any Internet enterprise. But whether it's consumers or individual executives connected to their businesses from home on a broadband connection, any network, any enterprise, government, commercial, academic, non-profit, small or large, to me they're the same. So, I'm happy to talk about future trends in security as they apply to consumers.

Really two points and then some conclusions looking forward. First, transparency and integrity. George Will commented on NBC News many months ago at the beginning of the Enron/Andersen implosion, he said that what has to happen post-Enron/Andersen is restoration of transparency and integrity in the financial markets. And I remember all the day trading going on at the height of the Internet boom, I began to wonder how democratic, how open should the financial markets be. They're talking about extending the trading hours and all these virtual exchanges. They're still around, but the buzz is certainly gone.

But you got to wonder when institutions like that are called into question, when articles are circulating about

the SEC and conflicts of interest, what does that average American consumer, who can't read documents for the words like stakeholders, and they have to have that document, which I think is fine. You've got to talk the talk that your customer understands. So, who cares what they do or do not understand, you got to speak that language.

I think if people have faith in the Internet, look at the example of the financial markets, in the past seven years, of what technology has done to the financial markets. And if consumers are upset about the particular affairs of Enron/Andersen, there's a big challenge ahead for really imbuing trust, the faith of the consumer and the Internet, whether you trade online your stocks in your mutual fund or retirement fund is day traded still or whatever. As we restore, we as companies, individuals, with our wallets, and government regulators restore transparency and integrity to the financial markets and the accounting industry, I think we look to the Internet and the value of what happens on networks is the next big challenge.

There's a quote from 1986, Walter Reston, who was the chairman of Citicorp back then, during the time of the Latin American banking financial meltdown, if anyone remembers that. He said in a speech at Columbia University -- for those of you who have seen me speak before, if you're thinking, why does Peter keep quoting Walter Reston, well,

it's still relevant. What he said in '86 at Columbia University is still relevant today, so here it goes again.

He said that in the Industrial Age, money was power. In the 1980s where we had international finance, currency exchange, cheaper jet travel, the fax machine, international telephones, mobile phones, information about money was power. Clearly, today with the Euro and online trading and information about information about whatever -- that's my own theory -- information about information about whatever is the power.

So, if we are in a little bit of a pick-up period of transparency and integrity in our financial networks, I think there's a huge Grand Canyon of problems when it comes to transparency and integrity in the security of our information networks.

But the fact is, my point is simple, that power of the information networks is going to be more valuable and more significant than the money traded through our traditional and Internet-based financial networks.

So, the second point I want to make is that the burden does not fall to the consumer. There are points about these different policies about what consumers can do. Well, there are firewalls. You know, I've been online since 1986 and I can't deal with upgrading anything. I'm not proud of that, but I've got better things to do with my time. I

want stuff to be simple, Commissioner Swindle, I take that point, and transparent. I don't want to worry about security as the consumer. I don't want to think about it. I don't want to configure anything.

So, the burden falls to the owners and operators of the networks, as it should, because it's their assets fundamentally. If they don't take care of it, they'll be regulated, or more importantly, they'll be put out of business because security is now a competitive positioning point. If you don't secure your offerings to your consumer, you won't be in business much longer. Your shareholders will sue you. Your partners' customers won't do business with you or they'll sue you, and customers won't come back or they'll sue you. I'm a lawyer, so I have to throw that word "sue you" in a lot. I don't practice anymore.

So, when the burden falls on the operator of the enterprise or the network, one question, do you know what has happened in the network?

All right, I'll go to the Enron CEO. Do you know what your cash balance is today? So, he'll go to his accounts and he'll go, we don't know. That's pretty damn sad. But if you go to any CEO and ask what the cash balance is, they better damn well know, in real time, what their cash balance is, otherwise they can't make payroll, they can't pay taxes and all kinds of bad things happen as a result of that.

Of course, any CEO has an investment in the office of the Chief Financial Officer, internal auditors and accountants, external auditors and accountants, that software, hardware. A lot of money is tied up in making sure they know where the money is.

Is the same thing true with your network assets? No. Richard Clarke said at the RSA Security Conference in San Jose, California back in February that a Forrester report indicated that companies spend more money on coffee and doughnuts than IT security, and despite the egregious headline in U.S.A. Today yesterday, that companies overspend on IT security or overspend IT, I think the simple fact remains that you go in any major corporation -- forget the dot coms -- you go to any major corporation, they've got manicured lawns, flowers, jets and all these things, golf courses. How much are they spending on IT and what percentage of the IT budget is spent on security?

Yes, they make mistakes, they may have overspent on Y2K upgrades and they may have overspent on trying to rebuild legacy systems to participate in the Internet boom, which is no longer there. Granted, maybe there's overspending. But the fact remains, as a percentage of overall capital spending, IT security is well behind coffee and very bad coffee.

So, to the point of cash balance, the question

today is, what is your network balance, what is the balance between good and bad traffic?

Every CEO, every Board of Directors must think of this every quarter, because I think what's going to happen, the previous panel about standards, I think this is -- we had in Y2K a movement to change the definition of materiality, to include Y2K, the definition of materiality with the SEC and what companies have to disclose in their filings to the SEC to participate in the publicly traded markets. Those companies who want to participate in the markets regulated by the SEC, transparency and integrity, to engage in that market, you have to provide information to your investors, institutions and individuals alike. And I think you have to disclose, as a material risk, what you're doing on security and privacy. That's coming down the road.

I was in Tokyo last September at the Information Security Workshop and I represented the Japanese Police Authority who said, in the surveys of the 500 networks, only 20 percent had a security policy, whether it was a binder on their shelf or a machine-readable policy injected in the network. Of that, only 20 percent updated on a regular basis, but networks are constantly changing. And of that percentage, only a handful had the CEO or Board engaged.

So, I think, as we try and get consumers more aware these days, we need to get CEOs really engaged in

governing networks, the security, the cash balance, the network balance. That's going to take several years. And also, it's a good time to start because networks are fairly unsophisticated. You have all these legacy systems that have been upgraded for the Internet. It's ripe for new growth, and we're going to see an uptake in corporate IT spending in a couple of years, because all upgrades the past several years have been aging and it's a normal cycle.

So, I think it's going to be market-driven out of either competitive reasons, upgrade reasons or attacking new markets. To some extent, things like the SEC disclosure rules, Gramm-Leach, Bliley, HIPAA, any move by the FTC or OECD or other standards, that may influence it. But fundamentally, talk to anyone in business, regulations aren't going to make the CEOs change their minds, unless they get hit with a lawsuit or an investigation.

What's going to make them invest in a top-down approach in information security that ultimately trickles down to consumers is, how does that help my profitability and how does it help my business continuity?

You can imagine Jeff Bezos and Peg Whitman going non linear if their networks are not running at 110 percent of expected behavior. If they identify a network service attack, any Wall Street analyst is going to start hammering them because they know that consumers can't get to their Web

sites to conduct transactions. And that will affect their revenue projections for that quarter. And I bet in their contracts, Amazon, eBay, have their telecommunication providers sign these serviceable agreements for liability, that if we don't have capacity and you can't back it up and we lose transactions, you're going to make us whole in that quarterly result, as a theory.

MR. EICHORN: Peter, can I ask that you wrap it up?

MR. HARTER: Yes, sorry, sorry. In conclusion, I won't go through all four points. This one last point, and it is a serious note. What does all this mean? What's the greater good of security? I'm an IT security vendor, I want people to buy my software. It's called capitalism.

But a lot of the terrorists these days tend to work in countries that don't have capitalism, that don't have laws, that don't really care about security, that don't have law enforcement, and we're seeing that increasingly as we try to invest through micro-finance, reduction of debt obligations of the open world, people trying to build systems, build societies, build communities, one village at a time, they're going to need security, they're going to need information and communication technology.

So, I think down the road, we're going to see an increasing intersect between poverty and security and a way

to make sure that we're not opening ourselves up, opening the cloud of the Internet up to attacks from these unsecure countries, and also enabling people to participate in the civilized world. So, security will be a tool for any consumer, here in America or in any country that doesn't have Internet access, to participate in security. It is an essential tool to participate in the civilized economy. Thank you.

MR. EICHORN: Thank you, Peter.

Scott Hatfield is next. Scott is Senior Vice President and Chief Information Officer of Cox Communications, and he's responsible there for the deployment of Cox's next generation IP platform.

MR. HATFIELD: Thank you. Let me just digress with you a little bit and share with you my perspective. I am the CIO of Cox Communications. So, my day job is taking a look at protecting our enterprise and applying some of the corporate security policies that we've been talking about here so far.

Over the last year, I've had an opportunity to take on a special assignment, though, which is deploying our new cable modem product out there. As a large cable company, we have over a million cable customers attached, and taking both of those assignments together has given me an opportunity to really take my expertise in running a

corporate IT environment and look at what that means for the average consumer as they attempt to utilize broadband technology.

So, what I'm going to do today is just really highlight, in kind of looking at emerging issues, what are some of the things that we see coming as the -- over the next couple years. Now, let me just start with broadband. Jeffrey commented on broadband ISPs a moment ago and I was really glad he didn't mention Cox Communications. It could have been one of the more dynamic --

MR. FOX: I didn't get to your Web site.

MR. HATFIELD: Yeah, I didn't think so. Which could have been an exciting panel.

(Laughter.)

MR. HATFIELD: But I think that there are some important issues in that area, and let's talk about three that we see are exploding right now. And first, let me just enumerate them for you. Broadband itself, I think, as the world drifts towards broadband, I think that will have certain implications. We see home networking as exploding over the next couple of years. As the broadband pipe becomes available, we're seeing high speed and always on become -- driving the use of home networking and we're seeing an increasing number of homes with more than one computer.

So, as people get access to high speed Internet

and as they grow the number of computers in their household, obviously, their use of home networking goes up and that drives a certain risk profile.

We're also seeing an explosion in the use of wireless networking, and I think when you take broadband home networking and wireless networking together, you see a very consumer-centric risk profile that needs a lot of attention.

So, let's talk about broadband for a minute. I think there was a lot of attention a number of years ago to concern over sharing the broadband connection, and I think over the last year, that has really diminished. The industry has adopted a set of standards that go by the name of DOCSYS (phonetic). In between the 1.0 and 1.1 standards of DOCSYS, we've really taken it so that we don't have to be afraid of monitoring the wire and secure the risks associated with people sharing a wire into their home.

We now have baseline privacy that has encryption and e-management and really we have managed to secure and encrypt the data that passes between the cable and the cable modem that would be in a consumer's home. So, we've got this link of high security and I think we need to turn our attention to looking at the security on each end of that.

That takes us to home networking. Broadband is powerful. One of the things that it does is being always on, it changes user behavior. So, if you have an always-on

connection, you're going to probably leave your PCs on all the time so that you can go and access that PC on a whim. The fact that you're broadband also means that you're connected for long periods of time, you're going to have an IP address that's going to remain on all the time. You have the potential for people to come to you and identify your PC much more.

So, the fact that it's connected all the time and people can get to it means that people, users, will change their behavior. If you have one computer in your household, you probably don't turn on home networking. But when you begin to share this line, you are probably going to open yourself up and start to share files and drives and printers within your home, and that provides an opportunity for the average consumer to introduce security risk. He may -- by inadvertently trying to share a device between two computers in his home, he may accidentally offer that file to the world, which, of course, is a scary thing.

Wireless home networking is obviously proliferating. The 80211(B) costs are coming down. the average consumer can go out and for around $200 introduce an access port and begin to use wireless networking in his home. I think the average consumer probably does not have an adequate understanding of the security implications of a wireless network. Unlike a lot of things, like a home

firewall where you can go and take it out of the box and the defaults are set correctly, most of the wireless technology is not set correctly.

So, for instance, WEB, which is one of the few security capabilities available in wireless, is usually not turned on when people go to the store and buy a wireless gateway.

So, we can have a very strong encryption all the way down to the cable modem and then a consumer can accidentally begin broadcasting his home network to the entire neighborhood by the use of these wireless access points.

So, we need to be particularly careful that when we understand a consumer is going to introduce these into his home and wants to use home networking and open up his drives, we need to be particularly concerned about that combination. So, one of the approaches -- so, those are some unique risks that we see emerging.

I think having listened to the discussion throughout the day, there are a number of approaches to addressing this, and at the risk of oversimplifying it, one would be to make it automatic. Can you go and can you put in place a security scheme? The consumer doesn't need to think about security.

Number two is to educate the consumer to go and do

something about home security, but I think one of the concerns that's been raised here today is, can you adequately educate people about sophisticated networking topics, and then can you motivate them to get up and to go do something about security, and I think that those are things that people have had limited success with.

One of the things that Cox is doing is taking a third approach, which is to offer a solution. So, for one of the first times that I'm aware of, Cox is introducing a home networking solution where we believe that people need a high tech solution, that they need to be able to talk to an individual and understand about the security impact.

So, we are beginning to launch a service -- and I don't want to turn this into a commercial, but I do want to describe the service to you -- sold in conjunction with our high speed Internet service. We will put a person in a consumer's house and they will drop off a firewall and a hub that they will then go to all of the personal computers in this consumer's home and correctly configure them, whether they be wired or wireless.

So, by the time our technician leaves the house, all the home PCs have networking available, they're all correctly configured with WEB and passwords and the operating systems, and then for -- on an ongoing basis, if there are any concerns about that home network, Cox will put a person

in the home to help correct that.

We believe that this is an important approach, that for the first time, I think we'll see professional grade networking brought into the consumer environment at an affordable price.

Now, I ask you to ponder for the minute, of the three approaches, making it automatic, asking the consumer to do something inherently very technologically sophisticated, or offering the consumer a solution. But this is something that we need to pay more attention to a viable alternative.

So, with that, let me just hit a couple of concerns that we have going forward. We do believe that delivering professional services into the home is the right way to go in the long term. We are concerned about some things that the average corporation has that the home does not have.

So, for instance, in a corporate environment, you set standards and controls around passwords. In a consumer environment, that's not possible. And in the corporate environment, you might be thinking about standardization, so you might only have one route or vendor. In a consumer environment, there will be dozens because of the number of consumer electronics offerings out there.

And in a corporate environment, you, from the very first day of install, begin to think about future upgrades to

that base, so that you know that as manageability comes along, as new security threats come along, you'll be able to react and upgrade and address that.

Those are issues that we need to pay more attention to in the consumer environment so that years from now, as these devices are out there and have become obsolete, we have ways of beginning to manage and upgrade and deploy those.

MR. EICHORN: Scott, is this a good place to wrap up?

MR. HATFIELD: Yes, thank you very much.

MR. EICHORN: I've been ruling with an iron hand here today, so sorry about that.

Alan Paller is next. Alan founded the SANS Institute in 1992 as a cooperative research organization. I think most of you are familiar with SANS. And Alan is responsible for the research programs there at SANS. Alan?

MR. PALLER: Thank you. Boy, SANS actually -- you know us as the people that put out the weekly news reports, but SANS is actually the principal education organization for people who are already employed in security. About 12,500 people spent a full week in immersion training last year to be the intrusion detection analysts in the military and to be the firewall people and to be the people who harden systems. That's what SANS does.

My role in it is the other part, the weekly summary of all of the security news. That goes to 160,000 people. And the weekly summary of the new threat, which goes to about 110,000 people.

I'd like to start -- and on behalf of the 30,000 SANS alumni, I really want to express my great admiration and congratulations to the FTC, and especially Mark and Ellen Finn and Laura Berger and Jessica Rich for bringing together such a wealth of knowledge and a breadth of interest. Beginning with Dick Clarke's extraordinary opening talk, every session brought new ideas, new examples, new energy and new insights to help small business and consumers deal with this scourge of cyber crime.

And in particular, I want to applaud Commissioner Swindle's leadership in this area. You've taken the lead for a long time. You've carried the ball alone and you're focused on -- you stressed that simplification is something we all need and I think we can learn from, and your spending the entire two days here with us is above and beyond, and it's very impressive that you did that.

For me, the two days revealed several fascinating facts. Dick was -- I've heard him talk a lot, but that was just an extraordinary talk. Those of you who didn't hear it, if there's a tape of it, go get it. It just really shaped and -- there's a lot of things I got out of it. But one of

the things was there are three areas, more, but three key areas that we can focus on for protecting consumers and the small businesses.

One is better education, better security education, so we act on our own. Two is better services from the ISPs, so they do a better job. We kept talking about only one in 10 were doing anything, it will be two in 10 now. And better development and security configuration of patching from the software vendors.

I'm a really strong supporter of education. We funded a project with the FBI that Governor Ridge awarded on the 18th of April. Six students from all around the United States had won a poster contest for kids improving security, and they were wonderful posters. I think AOL has a poster that we haven't posted on our Web site. But hundreds and hundreds of schools around the country competed. Next year it will be thousands of schools competing. So, the kids do things to promote security.

But the data from Tatiana at AOL, the data from Jeff at Consumer Reports, the data from Rob at Jupiter says that despite universal coverage of the problems of viruses -- I mean, it was universal, you had to be dead to not get data on Code Red and Melissa and the others, a shockingly high percentage of consumers don't exercise minimum security care.

And moreover, despite the claims by a couple of

speakers that the technology industry is doing a good job, Rich Pethia, who will speak next, gave us a memorable analogy that scotched that claim. He said -- I hope I remember it right -- security from the vendors was as easy to use as seatbelts that were hidden in a compartment in the trunk, and you could open the compartment only if you read the entire user manual. Rich, was that close?

MR. PETHIA: Close.

MR. PALLER: So, even if we do a pretty good job of educating the consumer, even if we do a pretty excellent job of educating the consumer, I don't think that option's going to be sufficient. It will take the rest of our lives and I don't think it will be enough. And the other side of protecting the consumer is the data that the consumer puts not on the wire, but at the sites that accept their private data, the hospitals and at the credit card companies. The Visa program's wonderful. It's not universal. But it is wonderful.

But we learn from Marc Zwillinger that liability -- and from -- oh, who's -- what's her name? Kimberly, thank you. And from Kimberly that liability is on the horizon. We can all decide we don't like it and it's still on the horizon. And -- but the new thing I learned was that the Gramm-Leach-Bliley and the HIPAA regulations and FTC's new regulations on the -- a few weeks ago actually provide new

standards that can be used for evaluation in those kinds of cases.

And from Frank Reeder, we learned that the Internet security -- Center for Internet Security has free tools that actually let companies measure the level of security of their systems so people can measure them against minimum benchmarks. So, we've got that. But several panelists told us, Scott Charney in the lead, that we shouldn't blame this one on the user. He's argued eloquently that it was the products and services that had to change, and to make security easier to use, we had to make it transparent. He brought us a breath of fresh air, I think, from that part of the country.

So, where does that leave us? If consumer information and systems are to be protected, we're left with the other two options, the ISPs doing more and the software vendors doing more, and the question is, what will cause them to act now? We can say, what will cause them to act in 100 years? And that's this wonderful pat them on the back, tell them they're good guys and hope that they come around.

The question is, what will cause them to act sooner? And for that, we have Professor Mary Culnan to thank. Her plan was humiliation, which I think is a good one. But some other people had another plan which was the Volvo plan where security becomes one of the key factors in

consumer buying and manufacturers respond by competing to offer the safest systems.

And since this panel is on alternative approaches, I want to tell you about two -- real quickly about two alternative approaches, one well underway and one that will get announced tomorrow. The one starting tomorrow is called the Information Security Leadership Awards. It will be given at the Network Security Conference in Washington that Dick Clarke will keynote. Dick's already agreed to give the awards. The awards will recognize people and organizations that are doing a great job of helping to turn the tide against cyber crime. We're not absolutely certain of the titles, but they're called Best Home User Protector, Best Computer Worm Killer, Best D-DOS Defender, Most Painless Patch, Top Gun for Lawman, that kind of thing.

There will also be some other awards that SANS won't have a lot to do with called the Internet Raspberry Awards, the Most Compromised Operating System, the Least Responsible ISP, but let's skip that stuff. Oh, also the nation with the highest number of attacks per capita.

And I hope the awards system will help educate consumers and provide appropriate incentives for vendors, but there's actually a much more important initiative that's already underway. And it's led by the National Security Agency and NIST and Frank Reeder, Center for Internet

Security, with help from the FBI's NIPC. It has no official name yet, but I think the most probable name will be the Consensus Assessment of Risk for Security. Anyone work out the acronym? CARS, hmm, okay.

CARS will make compliance with programs like HIPAA and Graham-Leach-Bliley and the FTC's new regulations more measurable and more rapid and cheaper. The FBI has demonstrated that financial institutions with Internet connectivity face certain risks. We don't need another risk assessment to know if you use a particular operating system, you're connected to the Internet, you know you've got these risks. So, that's a starting point.

You could also hire a consultant to tell you what you already know, but if there's a consensus on what we know, we don't have to start there. We can start with the consensus.

And then the NSA and NIST have come up with minimum benchmarks that allow you to block those vulnerabilities. So, now we have the FBI saying, here's a set of risks all of you have if you use these operating systems. NSA and NIST and the Center are saying, here's a set of things you do to block those risks. And then the Center for Internet Security has come out with free tools that measure it. So, I think you're going to see that as the beginning of a big change. That partnership between

government and industry will, I think, ultimately be seen as one of the most important initiatives the defenders have found to start turning the tide against the attackers.

MR. EICHORN: Great, thank you, Alan. I think Mary Culnan was squirming about that trunk analogy earlier.

MR. PALLER: Was it yours? Oh, that's why it was wrong.

MR. EICHORN: Rich Pethia was introduced earlier, as well, on the first panel. But Rich is at CERT and he's also on the Internet Security Alliance. So, Rich.

MR. PETHIA: I'd like to get sort of down to basics, maybe take a couple steps backwards before we come forwards again.

When you look at the whole security problem, it really hinges on two things, the information technology, because we're talking about computer security, and the way you use that technology, and those are the two variables that we have to work with if we want to affect some kind of change in the way things are done today.

In the short term, from the technology side, I think you're going to see over the next -- now to three years from now, that there will be a significant change in posture on the part of many of the product vendors to spend more time eliminating vulnerabilities from their products. I think the humiliation factor is now coming to play.

I think the liability war that keeps getting raised more and more often as we go into meetings is getting the attention of corporate CEOs in the technology producing sector, and I think if you look at the people on the front lines, the day-to-day work of dealing with security, most of it has to do with defending against vulnerabilities in the information technology products, and the whole task of upgrading software, getting patches, distributing them, ensuring that we distribute the patch, you don't wreck your system, et cetera, et cetera.

And I think that all of the people now who have been struggling with the problem for years are beginning to recognize that there's little traction to be gained from trying to automate much of that patch distribution process. It's just too hard, it takes too long. We've got to get at the root of the problem and the root of the problem is too many vulnerabilities in the products to start with.

And so, I think that's an emphasis you're going to see over the next three to five years, and I think we're going to make some progress there, because I know from analyzing the vulnerabilities, that these are not esoteric design problems. These are simply cases of weak implementation, bugs in the software, the kinds of things that good software engineering practice knows how to reduce by two orders of magnitude, if you just put some discipline

in your engineering process.

After that, however, I think we're still going to be dissatisfied with where we are. If you think today about what it takes to secure a system -- and, again, step back, you buy your system and then the firewall and then the anti-virus software and then the authentication technology and then the encryption software and then perhaps virtual private network in some applications, you have a highly trained set of system administrators, et cetera, et cetera, et cetera.

When you add up all the costs, what does it take to secure a system today, you recognize that that's a very expensive proposition. It's no wonder the corporate CEOs balk when the security managers come to them asking them for more money.

What other kind of product or technology do you use where, in addition to the base product, you have to go half again as much as your investment simply to secure it in order to prop up the holes?

That problem's not so easy to solve, because now we get into the issue of engineering systems for high dependability, high reliability, high security, those three factors, those three characteristics are inter-related. And we really don't have many of the engineering techniques that we need to have to build the kind of systems that we ought to have today and we will certainly need in the future.

So, part of this is a research problem. How can we begin to build engineering frameworks that allow us to build systems with dependability and security to the level that we need for the applications that we need?

Also, I think we're going to recognize, the industry's going to recognize that there's been a significant change in who their customers are. Ten years ago, 15 years ago when the Internet was beginning to get some traction and move forward, we still very much had a community where the systems were designed by engineers and they were designed for engineers. The primary customers of the Internet were the research universities, government agencies, the Department of Defense for highly technical applications, and we had products that were built for a very technically sophisticated user base.

Not true today. We don't have that user base today because we've expanded the application and the use of this technology. We've moved beyond the engineering community and we've made this technology literally available to every man, woman and child on the planet, and those people simply don't have the technical skills and won't have the technical skills. It's a fantasy to believe that we'll ever pull all those people up the learning curve to have the technical skills that they need to have to secure their technology.

So, what we need is -- what was addressed earlier is we need systems where security is transparent. It's as easy to use as driving your car. You know, you put the key in, you turn it, you put on the seatbelt and you go, and that's the kind of technology we're going to need to see in the future, and I suggest we're about 10 years away from that technology because, to some extent, we still don't know how to build some of it. But the market's going to drive that way.

All of us are going to become increasingly dissatisfied with the amount of work that it takes to secure the technology we have available today, and the industry has always been good at driving out costs and it will respond, but it will take some time to respond.

Going on to the flip side, moving away from the technology itself to the use of the technology, there I think we've seen a great shift in just the last couple of years. In 1989, the National Academy of Sciences produced a book called Computers At Risk, and it was a study on what could be done then to head off this problem that we're now all struggling with.

One of the things they called for was the creation of a set of generally accepted systems security practices. What we heard today is that finally, after these almost, what, 10 plus years, we're beginning to see action on the

part of governments to begin to work together to define these practices and on the part of various associations to turn those practices into standards. I think over the next four or five years, we're going to have this great cacophony that we now have all of these organizations that are basically doing the same thing. I think we'll begin to see that coalesce and come together.

I think it's fine right now, that we're at a stage where people are all going off, working with their own individual constituent groups to push these practices forward because, as we said earlier, about 90 percent of them were pretty much the same anyhow. But I think we're going to want to see a convergence of that over time, and I think one of the things that's going to drive us towards that convergence is the insurance industry.

This is a risk management problem. We have a mature risk management industry. That industry has yet to turn its full attention to this computer security problem. But as the costs go up, as liability becomes more obvious, as the damages increase, both consumers and producers will be looking for some way to offset that risk and the insurance industry is a good way to do that, and they're already beginning to take steps in this direction.

So, I think you're going to see, over the next 10 years, you're going to see a whole new generation of

technology that will make dramatic steps forward in helping us deal with this problem, and between now and then, I think you'll see some concrete specific steps to reduce some of the most egregious problems, and then I think you'll also see the maturation of the risk management industry and a set of risk management knowledge that becomes more widely used and more widely available.

MR. EICHORN: Thank you, Rich. Richard Smith is last and Richard is an Internet security and privacy consultant. He's also a magician because we were very strict about not having computer-driven presentations and Richard has gotten me to waive the rule. But as our last person, I guess we won't be setting a bad precedent.

(Laughter.)

MR. SMITH: Yeah, I'd like to first say thanks to Mark for indulging. But I feel a little bit naked without a computer when I'm giving a talk, so let me bring this up here.

What I want to talk about here for my few minutes here was the issue of security by design, which has really been hinted at a lot here already on the panel. I have to agree with a lot of things that have been said, that I think overall we're going to be looking from vendors for our security, consumer security of computers, particularly software vendors and ISPs.

I want to get some examples out here. We've heard over the last few days here a lot of discussions of computer viruses, and that's an area I've been looking at for the last three or four years. And it always bothers me because I think there are some fairly simple technical solutions to those problems. And I keep coming to conferences and I keep hearing about the latest viruses and, you know, why they're still going on.

So, I thought I'd show some examples up here of some stuff that has been done with security by design to make the situation better. I have a -- I'm running a Windows ME system here, and I like to live dangerously. I don't run anti-virus software, which might be a surprise to people.

In addition, I have a folder here. I also collect viruses. You know, they come into my computer and I like to save them around, and this is one example here of a folder that I had that I copied off here. This is the Klez virus, which has been going on for the last two or three weeks, and other people in the room may have received this. As you can see, I've got 44 copies of this here in about three weeks. You know, for somebody that gets 44 viruses in three weeks and to run anti-virus software, that's kind of strange. But let's take a look at why I don't particularly worry about it.

So, this is an example here of the virus, and I'm running Outlook 2002. When you look up at the top and it

says, this html message contains script which Outlook cannot display. This may affect how the message appears. That's sort of a funny thing to say about a computer virus. But what has happened is after the I Love You virus came out, Microsoft got pretty embarrassed and said, we've got to do something about our products so that they don't spread these kinds of viruses as much. And so, they've added in some patch features where they disable mobile code or script code in email messages, as well as delete attached executable files.

So, the reason I haven't run anti-virus software is, if we take Jeff Fox's figures from yesterday, 60 percent of viruses come in through email. Well, I just use Outlook 2002, which throws them away. And so, this one segment of the virus problem, we can go a really, really long way of fixing by incorporating these new technologies, you know, that Microsoft has provided. And Microsoft matters because, obviously, they have a large section of the marketplace.

So, this is Outlook 2002, so if anybody upgrades, they get these features. If you're running outlook 2000, you can download a patch from Microsoft to get these same security features, and it protects you against all or many of the viruses that are out there. I don't know actually of any virus that will get by -- any email-based virus that will get by this system. I can imagine some ways of designing one

that would get by this system, but I don't know of any known one.

The benefit of this kind of solution is, well, it's easy, it's automatic, and I don't have to worry about updating virus software or anything like this. But what it requires is sort of a little shift -- a little paradigm shift for programmers, who are the people that are designing this system; they think, well, I need to send around executable files because that's my job. I exchange program code with other people and everybody must need to do that. But I don't think that's true. Most consumers don't.

So, we have to come to the -- we do have to de-tune the software a little bit, but it's only going to affect a really small percentage of the people that are out there.

Another example here was the Melissa virus, which is one of the first things that got me interested in computer viruses. I won't run this. I won't open this document up, not because I'm scared of running the virus, but because it has a lot of nasty words in it and I don't think that's an appropriate thing to have here in the FTC thing.

But if I did -- I could open this up, and I did it last night on my computer and nothing ran. And the reason was is there's another improvement that Microsoft added in in Word, and this is in Word 2000, was that macros had to be digitally signed to run. And a virus writer, that would

require them, in essence, to reveal their identity in order to distribute a virus. So, they wouldn't go around digitally signing viruses because then people would find out who they were. So, this improvement came out in Word 2000 and we can see what the effect was.

This is a little chart here of the top 10 viruses in May of 1999, and this is a little bit of jargon here, but you'll see under the virus column here the names start with WM, WM and then XM and, you know, W95 and WM. If you look at that list, in that top 10 list, almost all the virus names start with WM and that means that they're Word macro viruses. So, something like seven out of the 10 most popular viruses in May of '99 were Word macro viruses. This data point was right after Word 2000 came out.

If we now look at -- we fast forward to this year here and we look at that same kind of chart here, what's popular, we've got our friend Klez here at the top of the list, we'll see it says all W32, W32, W32, and there's no WM, Word macro viruses on the top 10 list. So, we have a simple little change that probably almost no one noticed outside of the people in the security business that had a dramatic difference in the amount of Word macro viruses that are out there.

My understanding is they've dropped off something like 70 percent in the last three years, and this is sort of

another data point. So, technology can make a difference. There's just no doubt about it. And I think that's where security begins is security by design.

I don't normally do this, but I'll do a little selling here for Microsoft. I think Microsoft has gotten the message here with Bill Gates' memo. He didn't send it to me personally. I'm not on his email list, but it is floating around out there. So, I got a copy of the memo here that came out on January 15th where he does talk about these issues here, that Microsoft must do a better job at security, even sacrificing some functionality.

Now, I personally think that they don't have to sacrifice that much. In the examples that I've given, I think they've given up very little for a lot of security. The problem that he really has, though, and I think it's a warning -- and this is from my own background, which is as a technologist and a programmer -- is he's got to change the culture of programming in order to get security into products.

Because for most programmers, worrying about security issues -- I know this is a generalization, I'm sure -- is right up there with taking out the garbage. It's just not very interesting. And what you need to do is in a product development team, you need to pull in people who are interested in security and are going to drive it, and they'll

be the security people that worry about these issues. And a lot of this is now being done externally.

But he's going to have to figure out how to get his development groups to think about this every time they release a product. Because what we don't want to have happen, we have that Word 2000 example where the technology was added in four or five years after the initial release of the macro feature in Microsoft Word. What you really want to do is rather than having the development teams be reactive and see what happens out in the marketplace, you want them to put these features in the beginning. And so, you need people within the development team that are going to worry about this.

Hopefully, this memo, and Microsoft, will help that process along. Thank you very much.

MR. EICHORN: Thanks, Richard.

Well, I want to ask -- Rich Pethia commented on this in a way, talking about the difficulty of patching. We, in government, now have a contractor in place to keep our systems patched and find out what software we have and make sure it's patched and I was wondering -- this sort of ties in with the model that Scott was talking about as well: Is there some way that consumer security can be wholly contracted out so that some third party has the responsibility to take that role from consumers?

MR. HATFIELD: I can start. I'm sure there's other opinions, too. Certainly there are a lot of very good third party organizations who can provide what's now called managed security services and who can help organizations -- typically this is too expensive for an individual to do -- who can help organizations do a better job of managing the security of their systems. It's a wide range of services, everything from security evaluations sort of at the top end to lower level kinds of things, like implementing patches and then distributing them across a number of boxes.

What we're all struggling with is the fact that there simply is scarce technical resource today. We don't have enough knowledgeable technical people to do the job, and so, where these service companies get traction is they take the scarce technical resource and are able to spread it across a number of different organizations.

It's a way to go. It's expensive. It's an extra added service that you have to pay for, and I think long-term what we're going to want to do is improve the product so we don't need that service. But in the meantime, until we get there, it's a very valuable thing.

MR. EICHORN: Alan?

MR. PALLER: I agree completely. That is, it will be a while. In the meantime, two groups are doing a really good job. I think the virus vendors are doing an

extraordinary job of taking that pain away. They're not perfect but they're -- the little thing pops up on my screen and it says, I updated your virus signatures, that's a beginning.

For two years, I used to give a speech and every time a Microsoft official walked in the room, I would always stop and say, I wonder why AOL engineers -- I wonder whether AOL engineers are that much smarter than Microsoft engineers because AOL engineers are able to update 27 million -- it was smaller in those days -- 27 million PCs every day and Microsoft's users all have to do it themselves. And then with XP comes automatic update. The real sadness in that is that's an automatic update only if you buy their new product. So, that's a big frustration because there's a lot of us, 100 million of us, who don't have that product yet. But at least for the new ones.

And I think those -- that combination of the virus detection guys growing their services, the vendors providing automated update and the ISPs giving us filtering of email and other services they're not quite yet doing, but they will be doing over the next few months, I think that will give us a beginning of a response.

MR. EICHORN: Taking off on Richard's point, if security by design is extremely, extremely successful, how will that affect consumer's role in securing their own

systems?

MR. SMITH: I don't really see consumers having much to do with security at all other than, you know, just playing it smart about -- more like things that technology can't deal with, like who you give your credit card to and what hoax emails you respond to, these sorts of things.

But I think pretty much it should be like in my car, I mean, you know, I have to buckle the seatbelt, but I don't have to worry about the airbag, I don't worry about the crumple zones, I don't worry about the collapsing steering wheel, I don't worry about the steel cage, you know, all that stuff. So, there is some things I have to do, you know, in terms of security in the car, but it's not about the technology so much. It's more about staying alert, buckling the seatbelt and watching how I drive. So, that's where I would put it.

There shouldn't be settings that consumers have to fiddle with. I think that's the main thing that I would argue against. They're still going to have to be concerned about the con man tricks, they call them, coming in email. But I don't think there's a lot you can do about that.

MR. EICHORN: Jeff?

MR. FOX: Yeah, I was going to say what you said which is, I think that you still have to drive the car carefully and accidents still happen, people still get hurt

no matter how much safety we build in.

Also, I think in the area of virus that when we tested the anti-virus, although once they know about the virus, the anti-virus software is able to incorporate the signatures, we did a test with it where we gave them novel viruses that they couldn't have known about. Some of those were not caught, and there's going to be clever people out there who are going to be able to produce viruses in the future. Anti-virus software is never going to be perfect. So, that's another reason why good practice by consumers is always going to be important. You can't rely 100 percent on the technology.

MALE SPEAKER: I've got to address the virus issue because it's another one of my pet peeves. There's nothing intrinsic about digital technology and software that says these things have to be vulnerable to viruses. The virus problem we have today is the direct result of design choices that were made by the vendors when they produced the operating systems that they produced.

We have viruses today because operating systems allow the importation of software executable code from unknown sources to run in an unconstrained environment without any validity. An earlier speaker demonstrated with just some simple changes that problem goes away. And so, we know how to design systems that are much more secure or

virus-resistant than the ones we have today. We just have to put those practices into use.

And I -- but I do agree we will never build a foolproof system. There will always be some guy who's smart enough to figure out how to get into it. What we need to do is make sure that the consumer devices are engineered in a very simple -- in a way they're very simple to use and also recognize that the real risk to consumers is that somehow their machines are going to be used to launch some other kind of attack.

So, if we can protect against the real highly likely attacks, I think we solve 99 percent of the problem, and then the rest of it I think we just -- folks have to keep their eyes open.

MR. EICHORN: Peter?

MR. HARTER: Briefly, there is a report from the National Academy of Sciences, the National Research Council came out, I believe, in January, Herb Lin over there produced it, on change control misconfiguration. I think that, in addition to viruses, is probably the biggest problem facing both enterprises and consumers.

That if you don't properly configure machines, albeit they're very complex, and no matter how you come out on the upgrade issue, I think we have to be cognizant of the fact that these are complex systems where things do change

and you have to upgrade to the next version whether you like it or not or whether you can afford to or not. That is going to be imperative in the near term.

MR. EICHORN: I'd like to throw it open to questions now from anyone except people who I went to elementary school with.

(Laughter.)

MR. CLARK: Mark's referencing how long we've known each other. I'm Drew Clark with National Journal's Technology Daily. Richard, your comments on Bill Gates' trustworthy computing memo sparked an interesting thought, which is what about those who aren't working for a centralized top-down software company, particularly software programmers in the open source community, those who are writing Linux.

Could you also comment -- you and any others -- on the debate currently going on in the security community about how open security exploits and vulnerability should be and whether open source is better or worse from the standpoint of protecting against security exploits?

MR. SMITH: Yeah, there's some interesting debates on this open source versus closed source issue, which is the whole idea if you have an open source operating system that you have many eyes that can look for security problems versus a closed system where you just have the vendor looking at it.

On the other hand, open source does allow a potential attacker more information of how they can break into that product. So, I think it's a mixed bag.

I look at it just like at the bottom line, well, you take these two products and which one works better. I can't really -- I'm not sure if the methodology that you use to create the product is the overriding issue here. So, I just look at this from a practical matter. Microsoft has a 90 percent share of the operating system market, around a 90 percent share of some of the particular application markets. So, at least in the desktop area, they're going to be the ones who are looking for security solutions.

When we get back to the servers, the web servers that run a lot of the Internet, then things do change, and we can have that debate about open source versus closed source, but -- and I'm not sure how that's going to turn out, we'll have to see.

MR. EICHORN: I'd like to ask just sort of a fun question. If you all had a crystal ball, some of you have commented on this, whether it's biometrics or wireless or what, what the home computing environment's going to be like in five to 10 years and how people are going to be securing those systems. Alan?

MR. PALLER: I have just a little one. In August of last year, four Hewlett Packard Jet Direct printers

engaged in a denial of service attack against an ISP in either New Mexico or Arizona and took it down. And the reason I wanted to bring that up is that we don't think of a printer as a computer that would engage in a denial of service attack.

But the people who make the network interface cards that are manufactured by about three vendors all put on that card that all these printer guys buy, TelNet (phonetic), which is a highly open system, FTP, a password-free account and another account with a password you can't change, and that's a computer. It's a full-scale, honest to God computer.

And the only reason I'm bringing it up is your home -- you gave us a lot of years, you said 10, right?

MR. EICHORN: Um-hum.

MR. PALLER: Your home will have a refrigerator that you control by wireless, you'll have air conditioning systems you can control by wireless, you'll have door locks you can control by wireless, you'll have phone systems that are all wireless, all of those will have network interface cards in them and almost all of those are being designed by people who've never heard of Rich Pethia, meaning they don't have a clue what secure means. Open, open, open is their entire world.

So, unless somebody who is saying, hey, when you

promise a consumer a good product, it has to have a minimum, not open them up automatically to attacks. If you don't say it to them, they're not going to do it. So, we're going to have a home full of printer drivers that will be able to attack anyone.

MALE PARTICIPANT: The attack of the killer refrigerator.

MR. PALLER: The attack of the killer refrigerator, right.

MALE PARTICIPANT: Just to reinforce that, I mean, this is a palm phone here, so it's a complete computer that's programmable, plus it's a telephone. That's a bad combination, a computer with communication. That's what Alan's really talking about here is all these different devices are going to be computers that communicate.

And 10 years from now, when we have sort of figured it all out --

(Laughter.)

MALE PARTICIPANT: All we can say for sure, because of Moore's law, is that we're going to have a lot more computers that can communicate, many, many more, whether we get -- whether we sort of sort through all these -- you know, these bad security decisions in the cards, I guess I'd be slightly more hopeful, but I'm also worried.

MALE PARTICIPANT: I think you'll have computers

where you can say stop virus.

MR. EICHORN: You reminded me of -- well, Alan's comment reminded me of Dave Barry, the humorist, and he wrote about how his refrigerator may have a chip that would communicate with his scale and he said he didn't want his scale reporting to his refrigerator.

(Laughter.)

MR. EICHORN: At this time, I guess I would like to introduce Commissioner Swindle for some wrap-up remarks, and I really want to thank the panelists for coming today.

(Applause.)

(End of Panel VII discussion.)

CLOSING REMARKS

COMMISSIONER SWINDLE: This has been a remarkable two days, and I'd like to thank this last panel. It was certainly thought-provoking, as everything has been. In the process of thanking, I'd like to thank our air conditioning expert --

(Laughter.)

COMMISSIONER SWINDLE: -- who -- I mean, this is -

- you are the stout-hearted people here. I mean, you hung in here. My feet are numb. I don't know about yours, but I notice that nobody fell asleep.

(Laughter.)

COMMISSIONER SWINDLE: The only ones who left were those who had frostbite and had to go home and take care of themselves.

I want to thank -- I've heard a lot of commercials here in the last couple of hours for various and sundry companies, and I'd like to give one for the Federal Trade Commission. Mark Eichorn and Jessica Rich and Ellen Finn and Laura Berger put this together -- Maureen, I'm getting to her. Just an incredible conference. I think this is the first one -- we have lots of these things, but this is the first one I've ever sat through the whole thing, which says something about the level of work we have going on around here.

But it's heating up. We made friends with Senator Hollings one more time, as I noted in the Business Section of the Post. So, it will liven up. But it's just been a remarkable presentation and just great presenters. The topics were lively and thank you all for being engaged and thanks to those four that put this together. I had not forgotten Maureen.

Maureen and I got to know each other back in

December when we started working on this OECD thing. She knew just a little bit more about it than I did, but not much, and she has been remarkable. She's a great professional and it's been a real honor and a privilege and a comfort to work with Maureen because she's kept me out of trouble.

And then I'd like to thank a couple of people in my own shop. Allen Wiseman who -- raise your hand, Allen. Allen's leaving us here shortly. He's a Ph.D. out of Stanford in Political Economics. I think that's right, Allen, or is that close? Something like that. Public policy.

And Allen did an internship with us a couple years ago during the summer. He wrote a book while he was here on sort of a collection of studies and information on the Internet and various and sundry aspects of e-commerce and privacy and he got into a lot of that debate, and he's going on to Ohio State here this summer and begin his professorship, and I didn't say -- I can't say much about the quality of the school that he picked, but he's a pretty sharp guy himself. But he's been a pleasure to have working with us on this.

And Dan Caprio, who many of you perhaps know from your experience with Dan, Dan worked with me when I was Assistant Secretary of Commerce and Congressional Affairs,

and had he not come and joined my staff, I would not have come back from Hawaii to be in Washington, D.C. and put up with all this nonsense. Dan is just an invaluable asset in working with industry, and one of the things I tried to do when I came here, I said, we have to have the input of industry and the think-tanks and the civil society and all the voices have to come to the table, because we're government. We don't know it all.

I'm one of the few people that will admit that, but we don't know everything and your input from the various and sundry perspectives that you bring to the table are invaluable to us, and I think you've collectively helped make the FTC a better organization, and a lot of it has come through the channel of Dan Caprio and his knowledge and his contacts, and I want to thank all of them for their efforts.

Ronald Reagan once said that "there's no limit to what we can accomplish or where we can go if we don't care who gets credit for it," and I think this whole issue that we're talking about right now will depend more on how well we cooperate as opposed to who gets credit for being first. And if we can keep that in mind, we'll go a long way.

I had 10 or 12 pages of notes and I kept striking things off as Alan went down the summary and I wanted to thank -- is he -- there he is right there. He did a great job of summarizing. I do want to just talk about a couple of

things. Things that come to mind in listening -- and I won't go back and repeat the wonderful remarks of Dick Clarke and things of this nature -- but some things that pop out to me through this two days of discussion, we're still learning. That may be the understatement of the two days, we're still learning.

We've talked about the complexity of threats and vulnerability, the anonymous nature of the evildoers, if you will. It's hard to find them and it's hard to stop them. We talked about the lack of the general understanding of the environment by the consumers and home users and small businesses and even chief executive officers of large corporations who, I think Alan said, God knows we've got to get them involved and I have, for several years, talked about changing the corporate culture and, you know, we talked about a culture of security. I'm talking about the corporate culture and how it does things.

If CEOs don't pay attention, nobody's going to pay attention. If they pay attention, it's just like the Marine Corps. If the colonel says do it, believe me it gets done, and it's just the way it has to be. We have to have leadership. Corporate culture has got to change.

The need for deep, deep, deep education and making people aware of the world we live in today, just as President Bush has tried to make it evident to everybody, the world we

live in today is one where the threats are virtually impossible to stop, but by collectively being aware, we reduce the threats and the risks certainly substantially and the same way with this world of information technology.

We talked about better product design, designing in security, which I think is a marvelous idea. How we do it is up to minds far better than mine, but obviously Richard Smith's presentation, marvelous illustration of what technology can do and what it's doing.

Have we found the utopian solution? No. Are we going to find it? News for you, no, we're not going to find it. Go back to the aviation analogy. I'm trying to get us away from cars and elevate the discussion, you know, aviation, a little pun there.

But, you know, we started off many, many, many, many centuries ago, two people. There were only six on earth and two of them got mad with each other and one socked the other one, and he was bigger and he got away with it, until the little guy went over and picked up a club and knocked the hell out of the big guy. Well, the big guy said, well, you know, I got to do something about this. So, he learned to box and we got a little more sophisticated. And then it went up to, well, if he's going to do that, I've got to stand back because he's got a club now like I have and he's bigger than I am, so I'll get me a spear and I'll throw the spear at him.

Then the guy came up with a shield and you see it leapfrogging, the technology evolving. And for every remedy, there is somebody who is genius enough -- it just amazes me, and we see it all the time at the FTC, people with brilliant ideas and they spend them all on fraud. You know, someone said in one of the early discussions yesterday that all the charlatans -- they didn't use that term -- are still out there, the thieves, the hoodlums, the thugs and everybody, they're just using the Internet now to apply their trade.

So, it's changed. Educating people to this. As I said, it's deep, deep education and it's going to be a continuous education and it's an enormous project. And Mary Culnan said, you know, there's never been a grandiose, fully effective, comprehensive, big public awareness education program. And I don't know if she said it exactly that way. And it's daunting to think about, but it's somewhat -- have you ever seen the recipe for cooking an elephant or eating an elephant? That's a big task. You eat it one bite at a time. So, we've got to take one bite at a time on this thing.

I've forgotten who made the point. I think it was Simson Garfinkel. What a name. With a name like Orson Swindle, I can talk about his name. What a name, Simson Garfinkel. Who does that remind me of? You know, somebody.

But anyway, I think it was him that used the term -- and I may be wrong -- he said, we've got to demystify it

all. That is a marvelous expression. We really do have to demystify it all.

We have some tremendous challenges before us. Marty Abrams, always eloquent in his delivery, and just great ideas. I love to talk to Marty and listen -- more importantly, listen to him. He suggested whatever we do, we must avoid lessening consumer convenience. A beautiful point. Consumers want things convenient, so we've got to try to avoid -- whatever we do to solve this security problem, we must avoid lessening conveniences. We've got to make it user-friendly and we've got to minimize, I think, as he said, consumer interaction. And always there's going to be this tension between privacy and security going on. We'll have that debate till hell freezes over and I think it started here in the last couple days in this room.

(Laughter.)

COMMISSIONER SWINDLE: But, you know, we've just got an enormous task ahead of us and we have to focus on the habits and the behavior of consumers. If we don't think about that when we're designing these super-sophisticated, fun operating systems and games, if we don't focus on what consumers do, intuitively, they do things. Consumers are not very security conscious. And I'm not saying they're dumb. They're not dumb, they're darn smart. But they have habits. We all have habits. So, we've got to keep that in mind when

we do these things.

And Jeff Fox expressed a great deal of frustration, I think, that we don't have enough information. Jeff, you're exactly right. But he comes from, without a doubt -- at least in my wife's mind and mine, too, Consumer Report is a marvelous operation. I just love Consumer Report. I have never bought a car in my life that I didn't go get a Consumer Report first and start researching. Then I found Carmax and the marvelous information you get from Carmax.

But I would -- don't start expecting this industry -- this big word we've got here, information technology computers and all the things that that means. It's not going to be like the Consumer Report database on every model of car for the last 15 years and every maintenance report. I mean, that's grand. But we've only been working on that, you know, for seven or eight decades.

This industry just got started. We are in the embryo stages of all this, even though we're a long way down the road. We've just started, but more importantly, like the steel industry, we're sort of solid, another little pun there. Slow to change, big plants and everything. The automobile industry is pretty stable in a sense. It has aspects to it, physical aspects to it that we know, we know quality, and it has evolved and we've collected data and we

have this tremendous reservoir. We don't have that here because everything is changing so rapidly, probably the way the automobile industry did 70 or 80 years ago, you know.

So, we've got a lot to learn. And to take the airplane analogy, since Jeff mentioned it, Jeff, we do need to correct the ways we're doing it, we do need better supervision and monitoring and safety and all these things. The airplane I got shot down in -- I got shot down in 1966 flying supersonic, one of the hottest fighters going. It would fly 1,200 miles an hour and that's fast. Not as fast as some of your computers, but fast. I got shot down because I got hit underneath the airplane. And now, keep this in mind. This was 1966. People had been shooting down airplanes since 1917 when they started flying in World War I.

I got shot down because the aircraft was hit underneath. The engine was running like a Chevrolet engine. I mean, it was going like a house fire. The hydraulic lines that control the flight controls were underneath the airplane and they were ruptured. I lost all hydraulic pressure, so therefore, the airplane wouldn't fly.

Now, this is 1966, and we've got airplanes that go twice the speed of sound and when you think about it, where do airplanes usually get hit? Underneath. So, let's put the hydraulic lines that make it flyable underneath so it will be the first thing to go so the airplane goes topsy turvy and I

have to jump out of it.

After that episode, not my particular episode but the episode of Vietnam, we started putting hydraulic systems up on top of the airplane. We are still learning. That's my point. We are still learning in something even as sophisticated as the aircraft design business. So, we've got a lot to learn.

Peter Harter made, as always, great comments. Corporate executives have got to get engaged. If they don't get engaged, we're wasting our time talking to consumers. We're not really wasting our time talking to consumers because if we just took some simple precautions, we would solve 80 percent of the problems. We'll never get to that last 20 percent, but CEOs have got to get involved.

Are there deficiencies? You bet. Incredible deficiencies. We have to all work together, we've got to make improvements. There's a lot of improvements to be made. We've got to keep talking. We've got to keep the criticism going. I would contend that if we keep the dialogue going and it's constructive dialogue instead of litigious dialogue and everybody involved -- and this includes Microsoft will say, you know, you've got a point. We need to correct that.

We've got to get that going because we start squaring off and going to our different corners and coming out fighting, we're going to lose precious time and this

industry is moving at a great rate and we're not going to solve problems as fast as we can solve them, but we're going to solve them.

Education is absolutely essential. A culture of security, which I talked about, we must obtain that. It has to be intuitive. Privacy awareness -- keep this in mind, privacy awareness has taken us years to get the public involved. The public now thinks about privacy. Security may be more difficult to get the public involved than privacy. But for certain, they will get involved. Now, somebody talked about -- earlier about the hammer. They used the analogy of the hammer. And somebody said, companies are hesitant to get involved and spend the money on it because everybody's not doing it.

I would contend that the ultimate hammer came out of Adam Smith's hand. The marketplace is going to tell you you better damn well get serious about security industry. You've got to start designing in or designing out, maybe that's a better way, the flaws.

The market will dictate this. The market has now started dictating that you better take care of privacy matters. The marketplace will work because simply this, if you're in business and your consumers or your customers, more specifically, don't have confidence, if they aren't comfortable, if they don't trust you, you lose in a dynamic

marketplace. And this certainly is a dynamic marketplace, because people that we thought were great three or four years ago don't even exist today. It's moving very rapidly and you better satisfy consumers. So, we've got to all work together and we've got to learn from each other, keep learning from each other, keep the dialogue going.

Our challenge is, this education is just enormous. Someone mentioned the Grand Canyon and I remember the story about the guy who was touring the Grand Canyon and the National Park Service guy was there in his little Smokey the Bear hat and said -- you know, looking out over the Grand Canyon, it took four billion years for this to be as it is today. The guy in the back of the room said, hmm, government job.

(Laughter.)

COMMISSIONER SWINDLE: That's about what we've got to do with education. This education process is going to be incredibly difficult and we've literally got to get down -- I mean, look how old we are, we're an old bunch. We've got to get down to five and six-year-old kids as they start off, because they're starting off at those young ages now. It's got to be a part of indoctrination, if you will, to make it intuitive.

The Marines use an expression, gung-ho. Does anybody know what that means? Anybody have any idea? Have

you ever heard it?

AUDIENCE: Yeah.

COMMISSIONER SWINDLE: All right. It goes back to the Chinese, obviously, gung-ho. It means work together. It doesn't mean charge up a hill, go to the beer hall and drink too much beer and go out and scream, go out and chase girls. It means work together. And I think we should employ a little gung-ho here and get everybody working together and see if we can't work together and solve these problems as opposed to trying to get one up on somebody else.

It's going to be fun. Jeff, bless you. Don't panic. Nobody panic. We're having growing pains. We're evolving. We've got a long way to go, but we're going to get there.

And I'll leave you with one parting shot and I want all of you, when you walk out of here today and you get to the highway out there, it's very dangerous. Look to the left and look to the right and then you cross the street. Thank you very much for being a part of this.

(Applause.)

(Whereupon, the workshop was adjourned.)

C E R T I F I C A T I O N O F R E P O R T E R

CASE TITLE: CONSUMER INFORMATION SECURITY WORKSHOP

DATE: MAY 21, 2002

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

DATED:

_____

CONSTANCE A. STACKER WILSON

C E R T I F I C A T I O N O F P R O O F R E A D E R

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

_____

SARA J. VANCE