**FEDERAL TRADE COMMISSION**

MONITORING SOFTWARE ON YOUR PC:

SPYWARE, ADWARE, AND OTHER SOFTWARE

Monday, April 19, 2004

9:00 a.m.

Federal Trade Commission

Sixth and Pennsylvania Avenue, N.W.

Washington, D.C.

For The Record, Inc.
Waldorf, Maryland
(301)870-8025

1

2

3

# I N D E X

**P R O C E E D I N G S**

- - - - -

MR. PAHL: Good morning, and welcome to the FTC's Spyware Workshop. My name is Thomas Pahl. I'm an Assistant Director in the FTC's Division of Advertising Practices here at the FTC.

Before we begin our discussions today, I wanted to address some preliminary housekeeping items. First, I want to emphasize a few logistical points. We have a lot to cover at the workshop today. Our schedule is packed. So we're going to do our very best to stay on time. I would ask everyone to try to be back from breaks and from the lunch on time so that we can continue to keep pace with the schedule that we've set forth.

You each should have received a visitor's badge today when you came into the building. Please retain that throughout the day. If you take it off, you will have to get a new one and go back through the security procedures, and that will take some time. And also, wear your badge throughout the day when you're wandering around the building. It will help our security people here at the FTC.

Please turn off cell phones and pagers, because it may interrupt the discussions. Coffee is available outside in the hallway, courtesy of the On-Line Privacy

Alliance and the law firm of Hogan & Hartson. I want to thank them for providing us with coffee today.

You should have each received a folder when you arrived here today. In the folder, there's a list of local restaurants and lunch spots. The bathrooms are located out in the main lobby behind the elevator banks. And in case of an emergency, you can exit the building either through the front door, where you came in, or from the door on the north side of the building.

Second, I want to emphasize a few points about public participation in the workshop today. We have already received many public comments. And for those of you who have submitted comments, thank you. We have extended the deadline for submitting public comments until May 21st. And so if you hear anything at the workshop today that you'd like to comment on or would like to supplement a comment you've submitted in the past, we would appreciate it. You may submit comments to our box at spywareworkshop2004@ftc.gov.

There's a table in the lobby -- or actually, there are two tables in the lobby with materials related to Spyware. I would encourage you to pick up materials and make use of them.

Finally, the moderators today will be posing questions to panelists based on our review of the

comments that we've received and our review of other information that's been publicly available.

We also will try to pose questions from the audience to each of the panels. If you're interested in having a question asked of a panel or panelist, please write it down on one of the note cards that's included in the folder you were given today. And the cards will be collected by Shakeel Balroop. Shakeel is back dead center in front of me, and he will be collecting the cards during the panel presentation and throughout the day.

So if you have any questions, please write them down and give them to Shakeel, and we'll ask as many of those questions as we can. Please understand that given the tight timing of the workshops today, we probably will only be able to ask a couple of questions to each of the panels. But we will retain the questions, because they will be helpful in guiding our future analysis of issues related to Spyware.

Now, it's time to begin the workshop. The agenda calls for opening remarks by FTC Chairman Timothy Muris, but he's unable to be here today. Instead, we'll have remarks from the FTC's Director, Bureau of Consumer Protection, Howard Beales.

Prior to becoming Bureau Director in 2001,

Director Beales was an Associate Professor for Strategic Management at the George Washington University. During his tenure as Bureau Director at the FTC, the FTC has been involved in a variety of issues related to privacy, security and the Internet. We are fortunate that Director Beales is here to give us some opening remarks today. Director Beales?

(Applause.)

MR. BEALES: Thanks, Tom. Good morning, everyone, and welcome to our Spyware Workshop. I want to thank you all very much for joining us, and I'd especially like to thank the distinguished panelists for coming from all over the country to lend their insights and expertise on this very important issue as we address Spyware today.

For almost a decade, the FTC has undertaken efforts to address on-line privacy and security. Through many workshops and hearings on a variety of on-line issues, the FTC has sought to understand the on-line marketplace, its information practices, and the impact of these practices on consumers.

Through these efforts, we have brought together government, business, and consumers to discuss the issues, and to facilitate initiatives fostering privacy and security. Today, Spyware Workshop is the latest in

the Commission's efforts to understand and address another issue that affects on-line privacy and security.

Given the novelty of Spyware, little empirical research and analysis has been done to assess its prevalence and its effects in any kind of a systematic way. Anecdotes, however, abound. And the evidence suggests that consumers are worried about Spyware and what it may cause. Consumers have downloaded free versions of the two most widely-used anti-Spyware programs over 45 million times, and many Internet service providers have begun to offer Spyware detection capabilities to address customer concerns about such software.

Federal and state legislators are considering various legislative measures to respond to constituent concerns about Spyware. Governments, businesses, and consumers themselves are moving expeditiously to respond to the issue.

Despite the recent attention and efforts to address Spyware, many questions need to be answered. Perhaps most important, how should Spyware be defined? Should Adware be included within the definition of Spyware or not? Does Spyware collect and then misuse personally identifiable consumer information? Does the installation and operation of Spyware expose consumers

and businesses to security risks? And if so, to what extent? Does Spyware impair the operation and performance of consumers' personal computers? How difficult is it for consumers to uninstall Spyware?

These questions really just scratch the surface of Spyware. Today's workshop will obtain information and hopefully find answers to these and related questions. We hope the effort will inform the public debate over Spyware. We also hope that it will assist government, businesses, and consumers in developing effective and properly-focused responses to Spyware.

We planned six panels for today. The first panel will discuss the definition of Spyware and how Spyware is distributed, including the role of peer-to-peer file-sharing software in its distribution. Commissioner Swindle, who has led the Commission's efforts to promote security practices among both consumers and businesses, will offer some observations concerning Spyware and security risks, drawing on his experience in on-line security matters. Commissioner Swindle will be with us through the Miracle of Videotape.

The following two morning panels will discuss the existence and extent of security and privacy risks posed by Spyware, and the effects that Spyware may have on personal computer performance. To conclude the

morning, Commissioner Thompson will offer some thoughts about industry responses to Spyware, drawing on his own extensive experience in working with industry to address on-line privacy and other high-tech issues.

The discussion this afternoon will focus on how industry members, technology providers, government agencies, and others can work together to respond to the issues identified by the morning panels. After lunch, the first afternoon panel will discuss the measures that industry can undertake on its own or in partnership with government to address Spyware.

The second afternoon panel will inform us about anti-Spyware technology and improvements on the horizon. The final panel will address legislative, regulatory, law enforcement, and educational initiatives that the government could undertake to address Spyware.

Again, I would like to thank the panelists for their participation. We have over 30 panelists here today from all over the country, and they reflect a tremendous amount of experience and expertise. We look forward to learning from you, and we look forward to hearing from you about this timely and important issue. Thank you.

(Applause.)

MR. PAHL: Thank you, Howard. I'd like to ask

the members of our first panel to come forward, and we can begin speaking about the issue of how to define Spyware.

As Howard had mentioned, there appears to be substantial uncertainty as to what types of software are or should be considered Spyware. The term Spyware has been used to describe many different types of software -- Adware, Malware, Snoopware, Trespassware, and so forth. Indeed, one of the terms frequently used in connection with Spyware, Adware is itself a trademark term, unrelated to what we're talking about today.

Today we'll begin by discussing what our panelists think that Spyware is, and how it is disseminated, including dissemination through P2P file-sharing networks. This discussion should help us assess the impact of Spyware and the merits of alternative options in responding to it.

Before we begin, I'd like to introduce our panelists. To my immediate left, the new arrival is Ed Black, who is the President and Chief Executive Officer of the Computer and Communications Industry Association, an industry advocacy group that promotes open, barrier-free competition in the offering of computer and communications products.

To the left of Ed is Mark Bohannon, who is the

General Counsel and Senior Vice President for Public Policy at the Software and Information Industry Association, a trade association for the software and digital content industry.

Immediately to Mark's left is Marty Lafferty, who's the Chief Executive Officer of the Distributed Computing Industry Association, a trade association representing platform companies, content providers, and peer-to-peer operators in the distributed computing industry.

Continuing along the panel, to his left is Avi Naider, who's the President and Chief Executive Officer of WhenU.com, Inc., an on-line contextual marketing company.

And finally, on the end of our panel, is Ari Schwartz, who's the Associate Director of the Center for Democracy and Technology, a public interest organization that seeks practical solutions to enhance free expression and privacy in communications technology.

Welcome to our panelists today.

Our first question I'd like to pose to the panelists is that the FTC's Federal Register Notice tentatively described Spyware as "Software that aids in gathering information about a person or an organization without their knowledge, and that may send such

information to another entity without the consumer's consent, or that asserts control over computers without the consumer's knowledge."

I'd like to ask any of the panelists to chime in on what they think of the FTC's working definition of Spyware that was put in our Federal Register Notice, and particularly whether people think that it's too broad, too narrow, or just right.

MR. SCHWARTZ: I guess I'll start. In a lot of ways, the definitions of Spyware have been in the eye of the beholder up until now. And really, the focus has really been on not so much the technology, but in the feeling of the consumer of the loss of control. It could be that they don't know how the software got there, and that is what throws them off and feels as though the software has been spying on them. It could be that their personal information actually is being transmitted and exchanged. Or it could be that they have software, and they just don't know how to get rid of it.

And because of all this proliferation of definitions, all these different kinds of software that have been put together, CDT worked with a bunch of companies and other consumer groups to come up with a new set of examples of unfair and deceptive practices involving software. And we actually have them out in

front of the -- at the table right when you walk in, if you want to grab it after this session.

But we feel that this was really an attempt to -- let me first say that I don't speak on behalf of the working group. We're simply members, and we helped organize the group. But it was really an attempt to take the discussion beyond the definition debate and get at the actual bad practices that are going on today where we can take action. These are things that are being done by companies.

And rather than have a focus on trying to come up with some kind of definition before we can act, we can say, "Well, here are places where we know software is taking place, where fraud already exists on-line," rather than focusing on trying to come up with that definition, we can focus on the bad practices, that if they were to happen in the real world, we all know that there would be action taken against them. But because they're happening on-line, we feel as though we have to come up and start from scratch all over again with a new definition.

MR. BLACK: I'd like to endorse that concept. But basically, while it's useful for some purposes to have definitions out there, if we're talking in the regulatory and legislative world, the idea of trying to

create, in essence, an illegal category of product is very dangerous and has significant consequences.

What we do want to look at -- and there are certainly complex and contrary conflicting values which have to be weighed in dealing with this subject -- but we do want to try to focus on and identify that conduct which we find reprehensible, that we want to limit, and the extent to which we want to deal with different types and categories of conduct.

And we may find different -- clearly will, I think, find different levels of problems and different types of, if you will, public ills that flow from certain practices. And we need to, I think, approach this with a lot of care, recognizing we're going to be dealing with a multi-layered, different-leveled approach of what we want to focus on. And focus on the definitional, rather than on conduct and the underlying values, I think, is going to just send us in circles.

MR. BOHANNON: I want to commend Ari and the working group. I think they've put together a very good initial -- putting forward trying to, I think, help define this debate in a way that's meaningful toward getting out the unfair and deceptive abuses that I think all of us want to try to combat.

Our association has not yet signed on to this,

but we do think that there are a number of elements here that are a strong beginning toward looking at how to identify those practices that have been the most abusive, examine then what we can do under existing law, which I think is a very, very important issue, before we then start looking at major legislative reactions in a way that may have consequences.

So I think, Ari, I think you've done a yeoman's work here. We haven't quite signed on yet, but I think it's a very good beginning. And I really encourage everyone here to take a look at these actions, which I think in many ways get at what are the frustrations that both consumer users and I want to say business users have had that have motivated passage of legislation in Utah and consideration of legislation in states, as well as at the federal level.

MR. LAFFERTY: The DCIA signed on to the -- we've been working with Ari and the other 24 members of the working group. But we have signed on, and two of our members signed on as well who are active in that group.

As a trade association focused on developing commercial legitimate business use of peer-to-peer file sharing and endorsing Adware, which we see is very different from Spyware, we're more interested in the positive aspects of best practices, defining high

standards for what the industry should be doing, which kind of complements what Ari did with it. We're looking at the other side of it, the very negative, very bad behavior.

So for us, it comes down to a key issue from the provider's view of providing consumers with notice, full notification up front, giving them a choice, a clear, affirmative choice to accept the software, and finally, control. From the consumer's point of view, it's knowledge of what you're getting. It's an option to take an ad-supported version or a pay version and clearly see the difference. And the ability to change your mind. To be able to uninstall it during the installation or after you have had it for a time, and be able to do that very easily and simply.

So that's kind of what we're about, and we're interested in things like permission, the relevancy of the advertising, the attribution of the advertising, efficiency of delivering, and communication, sort of the positive aspects to complement the work of the working group.

MR. NAIDER: And speaking for WhenU, I can say that we're quite pleased that there's unanimity on this on the panel in the sense that we're also a member of this working group.

And I think Ari said it perfectly, which is that at the high level, definitions are often problematic. If you make definitions too broad, then you wind up not having specificity and not really being able to address improper behavior. If you make them too narrow, you could wind up ruling out or not anticipating how technology is going to evolve.

And what the CDT has done, along with the working group, is take a very pragmatic approach that says, "Look, what we're all trying to do is stop rogue, deceitful practices that are harmful to consumers." And the way to identify rogue, deceitful practices is to come up with specific examples. And by coming up with very specific examples, things like Browser, Hijacking, things like Home Page, Resetting, things like consumers having applications that show advertising that do not identify themselves, no idea where it's coming from, no ability to control what's on your computer, we think that's the best approach in a very specific way to go after rogue and unscrupulous companies that do not adhere to standards that, you know, allow for notification, consent, and control.

So I think everyone on the panel, it sounds like, has come to the same conclusion, which is that the FTC definition is the correct definition. It may be a

little bit broad, and in that respect, establishing specific examples and standards is probably what's going to eliminate the bad behaviors in the industry.

MR. PAHL: I'd like to ask a follow-up question. I recognize the unanimity that we should focus on conduct rather than terminology or nomenclature. Nevertheless, there are some legislative efforts under way. There are a couple of federal bills that have been introduced. There's a law that recently passed in Utah to regulate Spyware.

And although we'll be discussing governmental responses to Spyware later this afternoon, I'd like to ask Mark to opine on whether the legislative definitions that we've been seeing out there are -- the legislative definitions and proposed legislative definitions are too broad, too narrow, or just right.

MR. BOHANNON: Tom, I think if you look at what has been proposed and enacted so far, to some degree, it reflects the earlier discussion in the opposite, flip coin perspective, which is I think you can get 10 people in a room and have at least, if not more, than 20 opinions about what Spyware is and about what the effects of those are.

As everyone knows, I think the one law that has gone into place, at least that I am aware of -- there may

be others, because this is fast-moving -- is the one that passed in Utah at the beginning of March. It was signed into law in March.

So far, the proposals on the whole -- and I'll talk a little bit about the federal -- have wanted to, I think, try to either regulate or stop the use of technology. I think, as the first panel indicated, it may be more productive and will be more productive if we look at how to stop the abusive and bad behavior.

I know I was in Utah several -- I see other colleagues here that were in Utah trying to work constructively with the sponsors of the legislation, with the Governor's office, because we're all committed to trying to stop those abusive practices that get in the way of effective experiences over the Internet.

For example, just to show you what the challenge is, in the Utah bill, Spyware is defined as any software that monitors usage of the Internet and transmits information back from a location. There are requirements for notice and uninstallation.

As we carefully looked at this bill to see what, in fact, it would do, we discovered that it was a very broad definition, that it brought into play and tried to rope in and regulate exactly the kind of software that many of us depend on for a confident

experience over the Internet.

One example is parental control software, which depends on children not being able to uninstall it, precisely what the Utah bill would have provided for. Parental monitoring in these situations is absolutely essential. And I think there was an excellent explanation by Net Nanny, one of the leaders in this area, explaining why there were extreme risks in the Utah bill, that their software probably would be the subject of litigation.

We also carefully looked at the implications of the bill and found that it probably had some detrimental aspects to tools that aid, in fact, in consumer protection law enforcement. For example, if one is potentially using web logs to check access to web sites, a modern security measure that many financial services and banks use to make sure that access is done right, that potentially was covered under this bill.

It also, I think, in our view, included routine benign Internet communications, including the underlying software for instant messaging. While it attempted to address only pop-up advertising, there were some very serious risks, are some very serious risks, that the bill also affects pop-ups that notify about legitimate needs.

I am an avid eBay user, for example. I think

that the way that the bill was talking about these kinds of pop-up-without-notice kinds of things would have affected those.

So I think what we saw -- and I want to emphasize, I think the response to the legislation had the right intent to try to get at some of the abusive questions that we're all trying to get at here. I think we look forward to working with them to make sure that we're really getting at those abusive actions, and not unintentionally affecting other software.

I'll just quickly say that at the federal level, there are some -- a little bit different approaches than what you find in the Utah bill. We have the Burns/Wyden/Boxer bill, S-2145. There was a hearing on this I believe at the end of March, early April. I can't remember the exact date. I believe March 23rd. Excellent hearing that I think thoroughly examined a lot of these issues.

That bill, in my interpretation, does not include a definition of Spyware. What it does is actually create across-the-board rules for all software, regardless of whether it is specifically in this category of what we were thinking about software or not.

The House bill, at least the last version that has been published -- and I know that there is further

work on it -- defines Spyware as any computer program or software that can be used to transmit from a computer and that has the capability of so transmitting information regarding the user of the computer, use of the computer that is stored on the computer, but also gives the FTC regulatory permission to distinguish Spyware programs from other commonly-used computer programs.

Again, I think the motivation of the sponsors of the bill are right on, that we have some abusive practices that we need to address here. But I think the difficulty in trying to legislate these definitions, as shown through both the enacted Utah laws and the other proposals -- and there are proposals in California as well -- show that it's going to be, I think, really hard to try to get at what we're all trying to stop here if we go down the path of defining the technology and regulating the technology, as opposed to coming to a consensus about how we make sure we address the abusive, deceptive, and unfair practices.

MR. PAHL: I'd like to invite any of the other panelists who'd like to weigh in on any of the definitions in federal or state laws that they've seen.

MR. NAIDER: I think what's happened is there has become a little bit of confusion this entire debate over Spyware that has actually affected some of the

legislation, particularly at the state level. And let me give you a little bit of history here.

When the term Spyware first became used on the Internet in the mid-1990s, it was used very specifically to address software that was installed on consumers' computers, typically without their knowledge, and typically that was recording or monitoring aspects of their behavior, or using the resources of their computer. And that was the industry definition of Spyware that was set in the mid-1990s, or towards the late 1990s.

What's happened recently is that as other forms of software-based advertising have proliferated, particularly ones that have been perceived as threatening to certain types of businesses on the Internet and that have sparked some litigation and other things related to the protection of business interest, the definition of Spyware has actually become very, very complicated. Because it's now used to address not just programs that monitor or secretly record behavior, as was in the mid-'90s, but it's now used to try to be all-inclusive and threaten what are some very legitimate technologies in other types of software-based advertising.

And as a result, what has happened a little bit is that at the state level, particularly the Utah legislation which was passed, there has been, I think, a

bit of mixing of the issues. The bill's intention is very, very good. And in general, we and many others in the industry are big proponents of anti-Spyware legislation.

However, in this particular case, what has happened is that the definition has been used to broadly cover business interest from competition, as opposed to specifically address consumer privacy and consumer protection. And as a result, you do wind up with these situations in which nobody -- you know, everybody has a different definition of Spyware. It's almost lost some degree of meaning in terms of the debate.

And I think we need to kind of get back to a little bit of a very clear understanding of what do we mean by software that does actually interfere with user privacy? What do we mean by software that does do legitimate advertising? How do we make the industry understand the definitions such that legislation which is genuinely intended to protect consumers and consumer privacy doesn't wind up with a different result, and that is, you know, engaging in sort of disputes between business interest?

MR. SCHWARTZ: I'd like to just add as well that it's not just the definition of Spyware that's difficult. I mean, Avi was just talking about -- we're

talking about software running on the user's computer. When you're talking about -- I mean, some of the bad practices that we've seen are things that run on remote servers, and it's not installed on the user's computer. Then, you know, what's the definition of install? What's the definition of uninstall?

A lot of times -- I mean, I think we could all sit around the room and come up with a good definition of uninstall that would mean that it's removing the program from the user's computer. But what if that program shares components with other programs? Is it acceptable to leave pieces on, or do you have to break the other programs in order to really uninstall it? Or is it just disabling the program that we really care about?

All of these -- I think you can go through a litany of different kinds of definitions in this debate that are all very difficult to come up with precise definitions for. I think it can be done, but it's going to be a very difficult pass to come up with kind of consensus definitions.

MR. BOHANNON: And in the end, what does that get us? I mean, I think we're all trying to figure out how we can construct a legal framework using existing law and perhaps legislation. I think what we're seeing is that we're spending a lot of time trying to define what

is Spyware, which I think is a good educational experience. But I'm not sure in the end that it's really going to get us to stopping the abusive practices that we all want. And I think that's the value of this workshop and the discussion that the FTC has initiated.

MR. BLACK: Just one point. To the extent that it's going to be difficult to get definitions in this area, we all agree, we are at the FTC, and one of the issues, I think, before us will be the extent to which, without further action or a regulatory proceeding, the FTC can, if you will, whittle down at the problem.

And I think CDT made a very good presentation at another event to the extent that there is existing authority to deal with, basically, deceptive and misleading fraudulent activity.

The extent that we can take some of that off the table by using the existing authority, we will have at least a somewhat smaller problem that needs solving. And if it is more identifiable and smaller, we're less likely to screw it up as we try to solve it.

MR. PAHL: One of the most controversial issues that appears to have arisen with regard to defining Spyware is whether Adware is Spyware or not. I'd like to ask Avi and Marty to discuss what Adware is, including its costs and benefits for consumers, and whether Adware

should be considered to be a type of Spyware.

MR. NAIDER: Sure. Well, as I mentioned in the last response, Spyware was never meant to include software-based advertising, which is what legitimate Adware is. And very specifically, it's software on a consumer's computer that has been installed at the consent of the computer -- of the consumer, makes it very clear to the consumer what it's doing, can be removed easily by the consumer, and effectively gives the consumer potentially relevant valuable information. Specifically, as the consumer traverses the web, software-based advertising can deliver things like retail coupons.

You know, if you visit, for example, the Staples web site, our software will deliver to you a $30-off coupon to use at Staples that you wouldn't otherwise know about. That same ability to recognize that you might benefit from a $30-off coupon at Staples gives the software the ability to deliver an advertisement for hotels when you're looking at booking a hotel stay in New York City, or an advertisement for a discount rental car when you're looking to book rental cars.

So in theory, the concept of Adware or software-based advertising is extremely pro-consumer. It's pro-competition. It's pro-competitive. And if done

with proper notification, consent, and the consumer's ultimate control over the computer, which is the key point -- and I think Ari said it before -- the consumer has to understand that they have this type of software, has to have the ability to remove the software, has to be made clear when the software is generating coupons and ads. In that case, you have a very legitimate, a very promising technology that actually promises to reduce prices for consumers and to make the Internet a more competitive place.

When done improperly, any type of software that's not done at the consent of the consumer, that doesn't make it clear to the consumer what it's doing, it monitors behavior, or potentially shows ads that are not branded, where the consumer doesn't know what they have, where the consumer can't uninstall, that would be Spyware, and it may fit that definition.

But it's very important to understand that legitimate software-based advertising, not only is it very clearly not within the definition of Spyware, but it's actually one of the most promising technologies that exists on the Internet today. And if allowed to evolve, it will make the Internet a very, very exciting place over the next decade.

MR. LAFFERTY: And I'll just add that there is

no overlap between Adware and Spyware. They're mutually exclusive. Adware is presumptively legitimate. It's a terrific business model for providing valuable software to consumers at no cost in exchange for accepting some advertising.

And the efficiencies are tremendous. If you compare it to broadcast television, where you may have 32 interruptions per hour of commercial messages, the typical leading Adware programs only serve up two pop-up ads per day. By using behavioral marketing to target exactly the right ad to the right consumer at the right time -- served anonymously, I'll add -- it's enormously efficient, perhaps 40 times more efficient than traditional banner ads in terms of the click-throughs, in terms of the performance of those ads for the advertiser, and also meaning the consumer has fewer interruptions.

So as Avi said, it's a terrific business model. It gives great value to consumers. And within the regime of notice, choice, and control -- I'll probably hit those again and again -- that's the key to good use of it.

Let me just add a couple of points in terms of best practices that we see as the DCIA. Two points in general. Consumers elect to install the software based on informed consent. Very important. Secondly, consumers receive a reminder disclosure during the

software's download installation, with an option to cancel. So they have the right to change their mind during the installation.

And then specifically with respect to Adware, the consumer receives an application that offers benefit and utility that they would otherwise have to purchase in exchange for accepting the advertising. The Adware providers prominently offer users access to more information and links to customer support during the operation of the ads, attribution of the ads of where they're coming from so you see exactly who's delivering these ads to you. They maintain a customer support function that's reasonably adequate to respond to ads. And finally, they brand their ads. They're listed in start program menus clearly. They're easily uninstalled with traditional normal ad-remove programs provided by the operating system.

MR. PAHL: Okay. Someone suggested that all software downloaded onto a computer without adequate consent of the user should be treated as Spyware. I'd like to ask Mark whether there are forms of software that are beneficial or benign that are downloaded without the consent of users.

MR. BOHANNON: Tom, that's an interesting question and a difficult question. Let me just say that

I think out of the discussion today, we've come up with some basics for making sure that there are some common approaches to this.

You'll notice that there is not one single element in any of those approaches that is determinative of whether there has been bad behavior or not. So I want to make sure that the issue of consent in and of itself, in my view, does not determine whether something is Spyware or not. I think we need to be very clear about that, that there are a number of elements here in defining bad behavior, which probably requires all of them.

The other difficulty -- and this gets at -- and the FTC has had -- some of us experienced a three-day workshop back in 2000 on this very question of what is, in fact, consent. I don't want to go into a great deal of detail here. All that information is still up on the FTC web site, and involves very complex issues of software licensing, both in a consumer and enterprise context.

But I think -- to show you the difficulty in answering this question, I have to ask you what do you mean by software in your question? Because when one, in fact, downloads an application, installs an operating system, uses an on-line service, including using software

as a service itself, there are hosts of pieces of code that may be accessed or used that are often necessary to the functioning of that program, and quite frankly, which the user, both in a consumer and in a business context, wholly expect to be there in order to make the application, operating system, or on-line service work.

Each of these are, in fact, software. Some of them might be stand-alone. Some of them might be components. Some of them might be protocols. Some of them might be APIs. This is a very complicated question, and I don't think there's any expectation that consent has to be given to each and every one of these.

So one has to be careful at what point and about what is the consent meant to be at. And I think that's why this workshop is so important, because it's not about whether there's consent at every stage, or whether there's consent across the board. It's about what is the meaningful consent that's relative to the promises that a company has made through their privacy policy, or went through other means to get at this.

So for example, you know, I'll give you my personal experience. I have Tevo. I get regular updates from Tevo. I don't consent to those every time they happen, but they're very important to me. My Internet access provider regularly updates my software so that I

have a more meaningful experience. I don't always consent to that. But I want it, and it's totally necessary to the functioning of my service.

Similarly, upgraded some software. Quite frankly, many security issues come into play here.

So I think one has to be careful about saying that there's any one element that is determinative of what is Spyware, and that you've got to look at the entire picture to make sure that we have something that is both intended to protect the consumer, but also to be consistent with what they expect in their experience over the Internet.

MR. SCHWARTZ: Can I come back to the Adware?

MR. PAHL: Certainly.

MR. SCHWARTZ: Because I do think that there's a reason that Adware has gotten a bad name. And a lot of it has to do with the fact that some companies have basically decided that they will do anything they possibly can to get their software onto the user's computer, and that they don't really -- and we found that a lot of those are Adware companies.

For example, a lot of them -- and I don't think WhenU is one of these companies, but there certainly are a number of companies that a little bit of research will find you information about that use affiliates to get

software onto people's computers, and they basically say, "Any way that you get the software there, we will pay you for. We will pay the affiliate for." If it stays there for a certain period of time, or if you get a certain number of downloads over a -- at some time.

And they don't check up on the practices of the affiliate. And the affiliates will use basically any means that they possibly can, including exploiting holes in the browser, which is where the true drive-by downloads come from, where the users don't even see a box at all. The software just gets installed on people's computers. Or simply lying to the consumer to get them to download. "You need this software in order to use this web site." And so you click "okay." And these practices are being done by Adware companies.

And so therefore, when Marty says, you know, there's no overlap between Adware and Spyware, I don't think that that's true. There is certainly companies that are engaging in bad practices. It's not Adware itself that makes it a bad practice, but we have seen -- Adware companies seem to push the lines by using these affiliate kind of programs in order to make it happen.

MR. LAFFERTY: I'll try and clarify the definition. So our response to that, Ari, would be that once you're involving deceptive practices, it's no longer

Adware. I mean, definitionally, presumptively, Adware is legitimate. It subscribes to the regime of notice, choice, and control. On the consumer side, knowledge, options, the ability to uninstall.

MR. SCHWARTZ: But what may be legitimate software in one context, right, may move to this other context that is being forced down on the consumer. They get it without knowing it. In that context, then, it's clearly Spyware. So it's the same program, just a different way of the consumer getting the software.

MR. LAFFERTY: Which is not to say there can't be Spyware which involves ad support. I mean, it becomes Spyware once you cross that line. I think the FTC gets at it with their definition of deception, which is what we're looking at, which can occur when there's a material misrepresentation or omission of important information. And the key to determining when that happens, when a disclosure is necessary, is the context, the expectations, what the consumer expects under the circumstances?

MR. NAIDER: I think that both Ari and Marty are correct in that the same way that there are companies -- specifically, certain businesses -- that use this term Spyware to cloak a business dispute in terms of pursuing, you know, anti-competitive measures against technologies

that might threaten them, there are also companies that use the concept of software-based advertising, or Adware, to cloak themselves in a mantle of doing good when they're doing bad.

So at either end of the spectrum, you have ways of taking a broad term and using it incorrectly. But at the end of the day, you know, definitionally, the notion of having a piece of software that can show you contextual relevant coupons and ads is a very positive thing. Definitionally, the notion of having software that deceives you and causes you to lose control over your computer is a negative thing.

And what camp you fall into is ultimately a function of your specific business practices, which is again why I think the work that the CDT has done is actually wonderful work, because it's all about the specificity of the business practices of those at various ends of the spectrum within the industry.

MR. PAHL: Okay. Let's move on to discussing how Spyware is distributed to consumers, and I'd like to pose a question to Marty about that.

One particular issue that has drawn a lot of attention is the bundling of Spyware or Adware with P2P file-sharing applications. I'd like to ask you what Spyware or Adware is disseminated through bundling with

P2P file-sharing applications?

MR. LAFFERTY: And again, going back to the definitions that we put forth. All DCIA members, which include companies and their content, the P2P software, and service and support sectors, certify that they do not distribute Spyware. They don't endorse, support, condone, have anything to do with Spyware.

And further, the P2P software suppliers all provide an alternative to their file-sharing software, which is Adware-free. They provide a, you know, $29.95-per-year paid version which is without the advertising for those that want it. It's the right thing to do in the spirit of industry self-regulation, to take that approach. This whole area is a rich one for activities like that, industry self-regulation, to come up with best practices.

I will say that the adoption rate has been overwhelming. The file-sharing software has been downloaded close to 600 million times globally. The ad-supported version is enormously more popular than the pay version. It's too early to tell, you know, absolute trends, because these have only been out for less than a year, for the most part.

But the P2P software is Spyware-free. The ad-supported versions are offered as a clear choice to

consumers, and they have a choice to obtain a version without Adware. And that's the way the industry is setting itself up.

MR. BOHANNON: If I could just add to Marty. SIIA has a pretty unique perspective on peer-to-peer. We have an incredible love/hate relationship with it. On the one hand, peer-to-peer networks are a means by which our members' products are pirated. And as an association that goes back probably the longest in terms of combatting piracy, we see a great deal of our members' products being purloined through these meetings. We see how, in fact, tools like Adware can be used to support these peer-to-peer networks.

At the same time, our members are also using peer-to-peer networks in distributed computing for very new business models and very new ways of getting the tools that people want into their hands. We think that the kinds of steps that DCIA has taken to diminish the reliance on those kinds of Adware uses in support of peer-to-peer networks is very good, and that it shouldn't obscure that while there are aspects of peer-to-peer that are quite negative, certainly from an economic point of view, that there are elements that are very positive. And we see very new legitimate businesses taking off because of the use of those.

Certainly, our members have been using them and not relying on the kinds of invasive tools that I think we're trying to get at here. And it's important to keep in mind that there is a double picture here on peer-to-peer networks, and I think Marty laid out some good elements of that.

MR. BEALES: Also, to say something unique about peer-to-peer -- well, not unique. But we also find that it has become a symbolic category which has been used for, I think, other purposes, the people who try to defame peer-to-peer. It's tremendous technology with tremendous potential. We're very, very pleased with some of the responsible steps that have been taken.

You know, I think one simplistic way to understand peer-to-peer and why it is caught up in so many issues, from Spyware to piracy issues, is it's amazingly efficient. And so it's a multiplier factor of whether you're trying to do something very valuable or harmful. It is -- frankly, it's just such a multiplier.

And I have to comment as I'm hearing question after question. We're knocking down, basically, one straw man after another, and I think that's useful. But I think peer-to-peer as a focus of Spyware is exactly that.

MR. PAHL: I'm glad you like the questions.

Other than P2P file-sharing, are there other means that are -- I wonder if Ari and others could talk about other means that Spyware is used -- excuse me -- other means that are used to disseminate Spyware.

MR. SCHWARTZ: Well, I think from what we've seen, you know, bundling is the most common, and I think that's where the discussion comes in in peer-to-peer is that a lot of programs will get bundled in there in order for them to pay for the software. And the question is do the users really understand what's happening? Are they just clicking through because they want the end product, and not reading the disclosures, or are the disclosures really not there? And that's the discussion to have, rather than focusing on the kind of software that is being downloaded.

But we have also seen -- and this is where we focus in the working group's examples document, you know, examples of truly deceptive and unfair cases, cases where people are given misinformation. As I said earlier, you know, you need the software to download the site, and you don't need the software to download the site. There is very common practice on the web today.

Another one that we see today that if it happened in the real world people would be up in arms about is getting these prompts. You get 10 prompts, you

have to keep hitting "no," and they won't leave you alone until you finally hit "yes" and download the software. If people were walking around in the real world and were locked in a store until they bought something, you know, action would be taken immediately, you know? That's what it's the equivalent of, though, if you think about it.

And then, you know, these cases where they're taking advantage of security holes and downloading software immediately is -- you know, that's an ongoing problem with the web. I don't think it's going to stop tomorrow. The way to go after it is try and figure out exactly who's doing this, and try and figure out -- and make people see that if you do take advantage of these practices that are already illegal, that you -- and I'm not just talking under the FTC jurisdiction. I also mean under state fraud laws and under the Computer Fraud and Abuse Act. Let's get the Department of Justice involved in this as well.

MR. PAHL: Okay. One more question before we turn to some questions from the audience. And I'd like to ask Ed whether there are problems with operating systems that facilitate the dissemination of Spyware.

MR. BLACK: Well, a few comments, although this I don't think should be the focus of a lot of the attention. But there are some things.

First of all, operating systems are not absolutely unique. They do have some unique characteristics. But it shouldn't be viewed as a totally separate category. One thing I -- when we're talking about operating systems in the real world, we're talking about one particular operating system product. It's an operating system product. And I think that is where there is a point worth making. What we think of as operating system software, the actual code, which most people think is operating system, is one thing. The product that we have that we buy as Windows is something different. It is a lot of application software which is bundled in.

There are some significant aspects to that that may be worth pointing out. First of all, with regard to the extent that there is a security aspect which runs through the issue of Spyware, there is a real question whether or not some of the complexity created by that bundling of product-after-product, the constant expansion, the complexity of the product, will, in fact, make it more difficult to deal with some of the underlying problems.

Also, there's something I think people haven't thought about a whole lot. When we talk about -- and I think we all agree -- transparency, meaningful consent,

user empowerment, best practices, you know, and frankly, allowing technology to help solve some of these problems, are five things I've sensed that we all pretty much agree on. But when you deal with, for example, end user license agreements, if you're dealing with a very discreet piece of software, you may construct a ULA which permits or prohibits certain specific types of behavior related, really, to that product. And it may be that certain things which would be allowed, a certain amount of consent required, or how often you have to give consent can really be customized to fit different needs of the specific product.

When you start bundling software over and over, more and more into it, you basically wind up with, if you will, the lowest common denominator ULA. So your end user license agreement winds up being very restrictive, because you must meet -- you know, what any one part of the software program may demand, you've got to build that in. And then it applies to a lot of other parts of the large bundled product, where it really may not be inappropriate, it may undercut user empowerment.

And so I don't want to dwell on it too much, but, you know, informed consent and meaningful consent here is an important part of it. And to the extent that, you know, there are guidelines and concerns about the

nature of the click-on agreements that you have, I think you've got to worry when new products are getting massive.

With regard to -- and it's been mentioned already, but, you know, the browser, i.e, for drive-by problems, is a serious problem. Whether or not it would be as much if it were bundled or not bundled the way it is, you know, we can debate. But certainly, competition in the browser area to help deal with that would be one. Active X on many of our units, much less secure than some alternatives.

So all of this intertwining of security throughout the issue of Spyware is something we've got to be aware of. Because to the extent that we can define certain things as improper, as legal, that's great, and we can try to enforce them. But to the extent that the vulnerabilities are there and can be exploited by those who will be hard to catch, that's part of the problem.

I may submit, if you want, for the record, this is on cyber and security, a paper which we did by some of the leading technology experts which lays out some of the specifics relating to the operating system and how it might apply. Thanks.

MR. PAHL: Thank you. Before we turn to questions from the audience, I'd just ask any of the

panel members if they'd like to offer any other thoughts about defining Spyware or how it's disseminated before we move on to the questions.

MR. NAIDER: I'd like to offer one final thought, because I think, again, many of the members of this panel are probably coming from a similar -- slightly different but generally similar perspectives. In looking at the panels that are to come later in the day, I think you're going to see many folks coming from very different perspectives. And I think it's important to anticipate again a little bit of that, and to make it very, very clear -- and I think we should all make it clear -- what it is that, you know, when someone comes and talks about Spyware or software-based advertising, what are their interests. Because at the end of the day, there's a lot of confusion on this topic.

Specifically, there are companies out there who simply feel that it is wrong to have software on a consumer's desktop that if you visit the company's web site can show an alternative offer to a consumer and alert the consumer to maybe getting those same services for a discount elsewhere. And, you know, it's a well-known fact, and there's a lot of litigation over this issue.

Obviously, we and many folks on the Internet,

many folks like, you know, the Electronic Freedom Frontier and others who are in favor of pro-competition, pro-consumer, feel very strongly that this type of technology is very promising. I think it's very important that we all recognize that in this context of Spyware and anti-Spyware legislation, those two issues should not be confused. Folks should be very candid when saying what the interests are that they're representing, whether it's a business interest that doesn't want competitive technology that may threaten the business, or whether it's a legitimate pro-consumer, pro-consumer privacy protection. Because otherwise, the issue just gets very confusing, and it's very hard to pinpoint anything and come to any conclusions.

MR. LAFFERTY: Just briefly, the copyright infringement issue is clearly the larger problem for P2P file sharing, and one that we're addressing and working hard with DRM companies and acoustical fingerprinting companies and content rights holders to get them to license their content and legitimize that aspect.

But even the Adware issue where -- for example, Gay Network, which is one of our members, has 43 million users, and from its inception, has only had 10,000 complaints, something like that. One tenth of one percent of the users complain. But they're still not

resting on their laurels. They've just recruited Reid Freeman, who is a well-known privacy expert from the FTC, to join their company next month, and will continue to improve their efforts to make it an even more user-friendly and effective experience.

MR. BOHANNON: I just want to, at least for me, summarize what I think this panel has demonstrated, and I think it represents our views, having worked on both the Utah, federal, and then looking at the California legislation.

I think the effort to try to define Spyware is a very good educational effort. I think it has helped inform people about different kinds of software that is out there that is both important to the function of the Internet, to a positive consumer experience, but which can also be quite invasive.

I worry that if we continue to focus our efforts on trying to come up with a legal definition of this and regulate it accordingly, that in the end, we're not even actually going to get at the bad actors. We're probably going to get at the good actors who are trying to do the right thing. And I think that this highlights that we need to focus on how to come to a consensus on how we'd legally prescribe the abusive behaviors that I think were described here today.

So I think this FTC workshop has been very important in terms of focusing that attention on what is probably, in the end, the more productive approach, rather than something that we're going to spend a lot of time doing, and in the end, may not satisfy anyone.

MR. PAHL: Okay. I'd like to pose the first question from the audience. And although it's not so identified, I am sure that Avi will want to respond to this one.

"The FTC says Spyware is software installed without a user's consent. PC Pitstop research shows that over 80 percent of users are not aware it is running. By the FTC's definition, then, isn't WhenU Spyware?"

MR. NAIDER: I'm not sure that the PC Pitstop refers to WhenU specifically. I haven't seen that information. But just answering the question in general, there are certainly software applications out there that are not installed with user consent. We would agree to it. Very specifically, it's all in how you do it.

As Ari was mentioning before, a model in which a very clear disclosure is put before a user such that if the user even takes 12 seconds to read it, they understand that this software is being installed. And then similarly, even once on the desktop, every single time an ad unit is shown, it's branded. The source of

that ad is identified. It gives the consumers links to more information about the software and the ability to uninstall. And then consequently, a model in which tens of millions of consumers then do uninstall, it's clearly user consent.

And what I can say very specifically is in the case of WhenU, we've done over 100 million unique installations of our software. Eighty million consumers have removed it.

Now, what does that tell you? What it tells you is that we still have to make sure that the software that we bundle with is better and better value for consumers, because not all consumers want to see advertising supported by software if they don't value the software highly enough.

But what it tells you is that 80 million people can remove it. Clearly, 80 million people means that you have a mass market audience that makes a choice and makes a decision, and consents both upon the installation and consents on an ongoing basis to the software.

And by that definition, if you adhere to standards, it's a very consent-driven type of model. If you do not adhere to standards, you do not brand your advertising, you do not notify consumers where the advertising is coming from, and you don't let them

uninstall, then we would agree that you don't fit the definition of consent.

MR. SCHWARTZ: I do think that there is an issue in terms of bundling software, whether the consumers really understand what they're getting when they put it on, and also, of kids who download the software, and then their parents find out about it. I've heard from a lot of reporters, actually, for some reason, who have been telling me that their kids downloaded something. And then they went and found the stuff on their computer, and they were shocked that it was there.

And that's going to be common, also because of the fact that a lot of the bundled software programs will run separately from the original program, from the main component, that the consumer thought that they were downloading. So there's kind of a time disconnect.

And that's a high hurdle for the companies that are getting bundled in there to overcome. And, you know, they have to do a better job of notice at the beginning. They have to do a better job of explaining to people why they have the software and what it does when it's running, and the fact that it is running, and then making it easy to remove.

So it can be overcome, but it's going to be a very high hurdle for companies that kind of disassociate

-- that come bundled together, where the product is disassociated. We haven't done our own research on this yet, but, I mean, anything in the 80 percent sounds very high. If it's really that high, there is a major problem.

MR. PAHL: Okay. The second question is, "Wouldn't it be a better idea to regulate undesirable behavior, such as transmitting consumer's personal information and aggressively resisting the consumer's efforts to remove it?"

And I know we've talked a little bit about the first half of that question, you know, about regulating behavior, but perhaps panelists could speak to whether the ability to uninstall is something that -- how that figures into looking at Spyware.

MR. NAIDER: Well, again, I mean, I could address this very specifically. We absolutely believe that in order for something to be legitimate, the consumer has to have ultimate control over it.

And this is a really important point, because I think a lot of people forget that consumers install things all the time on their systems, not necessarily paying close attention. For example, anytime you buy a new computer, MSN.com right now is likely to be your home page. The reason that MSN.com is likely to be your home

page is because Microsoft has deals with most of the major computer manufacturers to set the home page of your browser to MSN.com.

Now, as a consumer, you may not know that or read it carefully when it's happening, but it's a fact. However, you have full control as a consumer to change your home page. If you don't like MSN.com, you can make it something else. You can set it to CNN.com, and many folks do that.

The point, and to address what Ari was saying, is that co-bundling and introducing one application into another application and disseminating it that way is, by nature, not a problem. For example, the Google toolbar is co-bundled with, or was co-bundled with, Real Network software just in the fourth quarter of last year. And there's no issue with taking one piece of software and putting it together as a package.

The issue is once it's on the desktop of the consumer, can the consumer, in case they didn't pay attention, in case it was the teenager who installed it and the parent who's now using it, can the consumer at that point understand what's taking place and make the decision to remove the software? And the only way you know that is if they can easily uninstall. If they can't easily uninstall, if they can't identify what the

software is doing, where it's coming from, then it really hasn't met this definition of consent.

And so, basically, we do think that the ability to uninstall, the ability to control your experience, is a fundamentally important part of this debate.

MR. BLACK: We'd actually second that, being very wary of absolutes here. But the ability to uninstall is, we think, very important, and in the bundle context, really essential.

MR. BOHANNON: I think the ability to uninstall is generally a right approach. One has to be extremely careful in this area, however. Because, quite frankly, an across-the-board technical ability to uninstall on the part of the consumer could, in fact, leave them in worse situations. And I think this comes across with regard to uninstalling security software, uninstalling computer protocols that allow you to interact with the Internet.

Ironically, if you give across-the-board ability to uninstall, we have got to have a very strong caveat emptor. Because many things are put in place to insure the continued functionality of software, and that the ability of a consumer -- and because I believe this issue is about more than consumers, but also about business users uninstalling. Just be careful what you're asking for here, because you could, in fact, lead to

greater frustration, less security, less ability to manage your personally-identifiable information if it is, in fact, a categorical right to uninstall.

This is a complex issue. And it is actually one of the reasons why we have yet to sign on to the Ari paper, because we think the issue is very complex. But I think that we look forward to working with the subgroup to make sure that we do have a common understanding of what it is that we want to be able to articulate as the uninstall concept without having detrimental effects to the end user and to the Internet community at large.

MR. SCHWARTZ: Again, I don't represent the working group. I'm just a member of the working group, helping to lead it.

The one point I wanted to get at in that question that I don't think anyone has addressed yet, and I don't know how people are going to react to it, is the privacy piece of that.

You know, we talked about behavior and regulating behavior. And CDT has said time and time again that the privacy issue is going to keep coming up and keep coming up every time that a new -- in new areas, and it's talking about new technologies, until we have an over-arching privacy bill. And the privacy bill is addressing, would be addressing, behavioral issues.

Again, that's something that's going to be hard to do, but at least we will be focusing on the direct nature of the problem, the behavioral problem here that's in place.

You know, six years ago, we had people talking about issues about tracking on the web, and then it was cookies following close on those heels, and then it was spam, and then it's Spyware. They all have a privacy component as a part of it. It's not a coincidence.

Two years from now, if we address part of the Spyware issue, another privacy issue is going to come up again. And again, you know, we'll keep saying it until it moves forward. But, you know, until we get that privacy bill moving forward, we're going to keep seeing the privacy issue come up in all of these technology discussions.

MR. LAFFERTY: Just to get back to the definitional question. If you focus too much on consent, it's clearly front-loading the whole issue through sort of the pre-installation part of it. And then if you go to uninstallation, you're talking about the end of the relationship.

I think we don't want to lose sight of the operational aspects of it. And Ari touched on it a little bit when he talked about the possible confusion

over pop-up ads occurring when you're not actually using the application associated with them during other aspects of your on-line activity.

So we believe it's just as important during the operation of the software to provide attribution, to provide links for more information, the ability to uninstall at that time. And you've got to look at this whole thing from pre-installation, that aspect of the relationship with the consumer, to the actual delivery of the ads, the serving of them, the operation, and then finally, the uninstall, which Mark talked about quite a bit.

MR. NAIDER: And just to sort of comment on what Ari said before, which is he made a very good point. We talked fairly little about privacy in the context of this panel. But the reality again, there's often a lot of confusion on that. Because downloadable software, even downloadable software that shows advertising based on consumers' interest, can be done with tremendous privacy protection.

And in fact, you know, one of our sort of hallmarks as a company is to show how that type of technology can be architected such that it is more protective than the way in which web sites typically do advertise. In other words, no use of cookies, no use of

server side profiling, no collection of personally-identifiable information.

And the thing that we predict will happen, you know, as Ari just said, is that ultimately, you're going to regulate behavior such that it's not a question of can you have software-based advertising or what type of software-based advertising, it's that if you violate the privacy of the consumer, that is going to be addressed very specifically through privacy legislation and privacy bills that address privacy violations specifically.

MR. PAHL: It looks like we're almost out of time. I want to thank the members of the panel today for a lively and informative discussion. I think we've heard a lot about how there's value in focusing on practices, not necessarily exclusively looking at definitional issues, and how we should be very careful in the terms we use as we move forward in this debate.

Thank you very much. We'll reconvene at 10:30, and I would ask that people be back in their seats at that time so we can get started.

Just to be aware, if you take off your badge, you've got to get a new one. If you go outside the building, you're going to have to go through security again, so please bear that in mind. Thank you.

(Applause.)

(A brief recess was taken.)

MR. PAHL: Okay, thank you. The next event on our agenda is remarks by Commissioner Swindle. Commissioner Swindle has focused on on-line privacy and security issues throughout his six-year tenure at the FTC. Since 2001, he has served as the head of the United States delegation to the OECD experts groups to review the 1992 OECD guidelines for the security of information systems. In 2004, Commissioner Swindle received the International Association of Privacy Professionals Privacy Leadership Award.

Unfortunately, Commissioner Swindle is not here with us today. But fortunately, he has left us some videotaped remarks to review. At this point, I'd like to task that the tape of Commissioner Swindle's remarks be played.

(Videotape is played.)

COMMISSIONER SWINDLE: Good morning, and welcome to the FTC's Spyware Workshop. Unfortunately, I am not able to be with you today, but I wanted to share some thoughts with you concerning the workshop, particularly on the questions that Spyware raises about on-line security and privacy.

The FTC is again gathering information about another Internet development and its impact on consumers.

It is proper that we do so as we search for appropriate courses of action.

Over the past decade, we often have used workshops and hearings as the first step in dealing with novel and evolving on-line technologies and practices. This collaborative approach in the past with industry, non-government organizations, and consumer advocates has resulted in our encouraging industry self-regulation, pursuing targeted law enforcement actions, making legislative recommendations, and using consumer education to address existing problems or those just over the horizon.

We have followed this model for many on-line technologies and practices such as on-line privacy, the on-line privacy of children, and spam. This workshop to learn more about Spyware is a continuation of this process.

The FTC has considerable experience upon which to draw in looking at the privacy and security risks that Spyware may pose for businesses and consumers. We have been in the forefront of privacy and security issues, working with industry to develop best practices, and bringing legal actions where companies violated their privacy policies or failed to adopt reasonable security measures.

The FTC has an aggressive track record of working with industry and consumer groups to understand and explore potential on-line security issues, such as workshops last summer relating to the protection of personal information and convening an on-line security advisory committee in early 2000.

We have undertaken a variety of consumer and business education efforts to promote on-line security, including the Dewey Turtle Comprehensive Awareness Campaign to help businesses and consumers become aware of security vulnerabilities, and how to provide protective measures and practices. Operation Secure Your Server is another example, an international effort to contact and educate operators of servers left open to unauthorized use by spammers.

With your assistance today, we hope to assess the privacy and security risk of Spyware. A survey of broadband users released last summer by the National Cyber Security Alliance found that over 90 percent of consumers have some form of Adware or Spyware on their computers, and most consumers were not even aware of it.

The next two panels will focus on the extent to which the increasing prevalence of Spyware poses privacy and security risk for consumers. The security panel will address some very important questions. For example, what

is the impact of Spyware on computer resources, and what effects does this have on a consumer's ability to use his/her computer? To what extent do Spyware programs hijack the browsers of computers? Do Spyware programs pose security hazards, and if so, what are they? Can Spyware capture a computer and use it for troublesome purposes; for example, to send out spam? Do Spyware programs, when bundled with file-sharing software, pose any unique security concerns? Does Spyware raise similar or different security risks for consumers than it does for businesses?

The privacy panel will discuss questions such as what type of information about users does Spyware collect? Is information collected on an aggregated or an individual basis? Is the information collected used primarily to display targeted ads? Is keystroke information being captured, and has it been or could it be used in identity theft?

The debate that has ensued around Spyware reminds me of the early dialogue we had about privacy policies. That debate, as you'll recall, was filled with lots of emotion and calls for regulation. The continuing and energetic dialogue among industry, government, and consumer groups has led to industry responding to the public's demand for greater disclosure and better privacy

practices and notices, without legislation.

Today, almost 100 percent of the most frequently visited web sites offer some form of privacy notice. Are we totally successful? No. Not by a long shot. But we are progressing. I believe we have made greater progress in finding solutions to privacy concerns than if there was simply static legislative attempts to address the problem.

As we go forward, we must keep in mind the unintended consequences of regulation. The challenge with Spyware is to seek effective solutions that address legitimate security and privacy concerns without unduly burdening legitimate software developers or hindering innovation.

This workshop is asking the right questions at the right time. I am confident that we will have a lively and informative discussion that will help government, industry, and consumers to find focused and effective ways to address Spyware.

I recall another lively workshop on spam. I must insist that there be no fighting among participants today. I would really hate to miss that.

Thank you very much.

MR. PAHL: Thank you, Commissioner Swindle.

Now what I'd like to do is introduce the

moderator for our next panel, and our panel will be discussing the security and PC functionality risks of spyware.

The moderator for the panel is David Koehler, who is an attorney in our Division of Advertising Practices, and I'd like to ask David to come forward, along with the panelists for our security risks panel.

Thank you.

MR. KOEHLER: Thank you, Tom. Good morning, and many thanks to our panelists for coming here to D.C. today on what appears to be the first day of Summer.

I'll start with introductions, very quickly, and there is more detailed bio sketches in your folders.

To my direct left is Maureen Cushman, who is legal counsel for U.S. Consumers at Dell, where she has regular contact with the tech support staff there regarding spyware related complaints received from Dell consumers.

To her left is John Gilroy, who writes the Ask the Compute Guy column for The Washington Post, as well as he is co-host of The Computer Guys' radio program on WAMU here in the District, and as such, he deals with many questions from consumers about spyware.

Next is Bryson Gordon, who is Senior Product Manager for McAfee Security's Consumer Division. McAfee,

as you all probably know, is well known for providing antivirus programs, and they have recently added anti-spyware capacity to their line up.

We are still missing Austin Hill, who will hopefully poke in and join us as the discussion progresses. He is co-founder and chief privacy expert at Zero-Knowledge Systems.

Moving down the line is Roger Thompson, who is Vice President of Product Development at Pest Patrol, which makes both a free anti-spyware program called Pest Scan, as well as a paid program that's called Pest Patrol.

Last but not least is Michael Wood, who is Vice President of Sales for USA and Canada, Lavasoft, who has been distributing anti-spyware products since the late 1990s, including a free program called Ad-Aware.

As Tom said, this panel is going to address functionality issues and security issues raised by spyware. When we say "spyware," we are still going to be using the definition that we were mentioning earlier, and that's the definition that was tentatively described in the FTC's Federal Register Notice.

With that caveat, I'd like to start by addressing the general kinds of consumer questions and complaints that you have been receiving relating to

spyware, and whether you see a trend here.

If we could start with you, Maureen. What has Dell's experience been in this area?

MS. CUSHMAN: Thank you, David. As David said, I am counsel for the Dell U.S. Consumers' section, and in that role, one of the organizations that I support is the U.S. Consumers Technical Report organization.

As many of you know, Dell is one of the largest sellers of computer systems to U.S. consumers. One aspect of its direct model is its direct connection with its customers.

Dell is uniquely positioned to share the voices of consumers about spyware related issues. We are going to share some aggregate data that we have noticed about consumer complaints around spyware.

One measure of the effect of spyware and the spread of spyware in U.S. consumer systems is a steadily rising percentage of spyware related issues of all Dell customer tech support requests.

Dell noticed this trend line about a year ago and started tracking it very closely. It actually became our number one call driver late last year.

Spyware related technical support calls have been as high as 12 percent of all technical support requests to the Dell technical support queue.

We are happy to report that some of our recent consumer education efforts seem to be having an effect. Consumers are learning more about this problem and how to get the full benefit of their Dell systems. We have seen a drop of about a third in these tech support requests related to spyware.

Nevertheless, spyware remains a huge technical support issue for us, and to add to what we perceive as our customers' frustration, our data shows that spyware related tech support calls tend to take a little longer than your normal tech support call to Dell. I think part of the problem is consumers are not yet able to articulate their problem is spyware, and so our reps must go through troubleshooting in order to identify the issue and help them solve it.

We found that the most typical customer complaints were where spyware ended up being the culprit relating to slow performance, inability to access the Internet, extra icons and pop up ads, Internet or system freezes, and so on. The number one complaint we hear from customers is they are noticing markedly slower performance from their systems. This makes up more than a quarter of all the Dell customer tech support complaints related to spyware.

Unfortunately, this complaint can easily and

erroneously be perceived as a Dell hardware problem and not a software problem. Certainly, this damages our brand and most importantly, prevents a good customer experience with our Dell customers.

We think this data represents and serves as evidence that consumers are definitely noticing the impact of this recent phenomenon on their systems.

MR. KOEHLER: Thank you, Maureen.

Bryson, I understand that McAfee has been tracking some of these complaints. Can you address that for us?

MR. GORDON: Yes, absolutely. First of all, from a technical support standpoint, just to follow up on what Maureen was stating, one of the interesting things that McAfee has been noticing is first off, for about the last 12 months, spyware has actually been a larger technical support problem for McAfee than viruses.

Customers calling in with complaints about a problem with their computer with a sort of marked performance degradation or inability to access the Internet, basically everything that Maureen was mentioning, a lot of people, because they don't have the knowledge to understand the sort of differences between what is viral activity and what is spyware activity, I mean those lines are becoming very gray.

When an user calls in, all they know is there is something wrong with their computer, and when our reps actually sort of take a deeper dive into what is actually going on, it turns out that between 10 and 12 percent of the time, it's because of spyware or adware, or some other what McAfee will call some potentially unwanted program being on that machine itself.

I think if we want to look at some of the stats that McAfee has been tracking, we can get those up there. First of all, with the McAfee virus scan, one of the things that customers can do is during the installation process, they can anonymously report data through an op in process, and based upon that, we have actually collected some very interesting numbers surrounding adware, spyware, keyloggers, dialers, exploit, and other things.

I'll actually go through some of the numbers which are actually fairly interesting.

If you look at the last eight months, the number of adware applications that McAfee has actually detected on an user's system is just under 40 million, with the spike coming actually just now in March with 11.4 million being detected on the user system.

One of the thing that is a little bit more disturbing is not the sort of traditional and sometimes

legitimate adware that is out there, it's some of the more malicious pieces of spyware, such as things like keyloggers. Even though we are not seeing huge numbers of keyloggers, the fact that we are detecting hundreds and thousands of them is still something that is disturbing.

This chart we have right now, this is actually the growth in spyware, adware, keyloggers, and various other potentially unwanted programs since August of last year, and it is showing that growth in things other than the sort of core adware has been relatively flat. However, when you look at the sheer numbers of detection, these have been normalized for consumer growth, for subscriber growth, but if you look at the sheer numbers, things like web dialers, the fact that we have detected 4.2 million web dialers in the past eight months, and when we have customers calling in telling us I have a $5,000 phone bill and I don't know what to do about it, it's showing these types of sort of non-viral threats are becoming a very serious problem for consumers.

The biggest issue is they don't know what they are. They don't know how they got on their system. Many people assume, because of the fact also in the last few months we have had so many major viruses, many people are just assuming that they in fact had one of these viruses

on their system, whereas, it's actually one of these non-traditional threats.

MR. KOEHLER: Bryson, did you want to go through any of the other slides?

MR. GORDON: Yes. If we go to the next slide, this is just showing the non-normalized figures, just raw detections. You can see just raw detections from August to where we are today, an upward trend in everything.

Even the exploit number, if you look at the number of exploits total, 13 million, and that is including things that will actually help spyware companies drop something onto the PC by taking advantage of a vulnerability in the Internet Explorer browser, and that can also include something -- there was an URL spoofing issue that was reported back in December, which I'm sure any people are aware of, and we saw an enormous volume of that particular exploit being reported. These things are being taken advantage of.

The next slide is just something to show what is the breakdown in current reported potentially unwanted programs, and showing that adware, which is still causing all the issues that Maureen mentioned, is right now the single largest issue that we are seeing.

MR. KOEHLER: Thank you.

Asking Roger and Michael, have these trends

been similar with what you have been seeing with Pest Patrol or Lavasoft?

MR. THOMPSON: I'd say it's very similar. So far, we have added more than we added in the whole of last year, in all categories. We are currently adding about 4,000 old fashioned pests a month, which is a lot, and they are not viruses. They are actually keylogger things, and we are adding about 300 adware a month.

In terms of performance -- it is appropriate for me to mention that, David?

MR. KOEHLER: We will get to that.

MR. THOMPSON: Absolutely, it's accelerating.

MR. KOEHLER: How about Lavasoft?

MR. WOOD: I concur. At least over the last month, we have actually moved into having to do daily updates instead of our usual frequency, which was about one reference file every three and a half days or so. We are actually seeing it now that we have to do multiple updates, and we are actually seeing where the companies are watching for it, putting out updates and putting out more updates.

MR. KOEHLER: To the panel, are these trends consistent with both consumers, private consumers, as well as business consumers?

MR. GORDON: I can comment on that. We don't

have specific numbers. All the numbers that you guys have been looking at are very consumer focused. I can state that just through contact with our enterprise customers, this is becoming an issue not just in the consumer area. Many, many enterprises are number one, spending money on anti-spyware, and number two, reporting it is a significant problem with employees.

I know that we have actually deployed our consumer anti-spyware application in various enterprises because of the fact that they really need to have some sort of protection immediately. It absolutely is a problem.

MS. CUSHMAN: To add to what Roger said, Dell has not observed the same sort of spike in business complaints that we have seen in consumer. It doesn't necessarily mean businesses aren't affected, but I do think perhaps they turn to their own IT departments or have additional security measures than your average consumer.

MR. THOMPSON: I'm inclined to think that businesses are probably as affected as consumers in terms of the adware component of this whole problem, probably not the traditional older kind of things. Corporations are probably pretty well protected against keyloggers and Trojans that some of the antivirus companies have been

helpful with to one extent or another for a long time.

There is no doubt that corporations are suddenly going on, hang on, what is out there, what is on my PCs.

MR. KOEHLER: Roger, what is the impact you are seeing on computer resources and is it a serious impact?

COMMISSIONER THOMPSON: Yes. Just as an example, I installed two clean images on two exactly identical machines, and measured how long it took to boot with my diagnostic software installed and adware was averaging about 150 seconds to boot. On one, I installed peer to peer Pest that ran on an average of 415 seconds, one I installed two peer to peer Pests, it runs out to about 890 seconds, just to boot. Web page access on my no adware PC, I could access a Web page consistently in four to five seconds. Once the Pest got involved, that was spinning out to 20 to 30 seconds for access.

Your computer feels sluggish and the boot time is just unacceptable.

MR. KOEHLER: John, are you receiving consumer complaints?

MR. GILROY: Yes. I guess I speak for the consumers and the people in the room here, I think. Everyone I've spoken to and gotten an e-mail from over the last ten years, they think this spyware drives them

crazy. It not only closes the system down, it can stop the system.

In fact, I've had readers come up to me and say their mouse doesn't work. I tell them to run a product and they will get rid of spyware, run their programs, and their mouse will suddenly work. These programs soak up resources to such an extent that it's driving people crazy.

Is it worth it, paying someone to come out to your house and spend $85 to clean the stuff off your machine?

In the last four or five years, I can almost graph the number of complaints I've gotten about products like this. We can spend an hour and debate the subtle differences between spyware and adware and invasive programs and malicious code and everything else. It's expensive. It's costing people money.

I was at a person's house on Friday, and they were saying instead of cleaning this thing up, I'll just buy a new system. That's where it has gotten to. It's gotten to somebody is writing code on the West Coast and there are hundreds of people on the East Coast that are so frustrated, what should they do.

My mom is 83 years old. She tried to install AOL 9.0 on her machine and she couldn't. Why? She had a

bunch of spyware running on her machine. If you call AOL, they will say, hey, first thing you do, get one of these detectors and then put in AOL 9.0.

It's a major consumer problem. I don't know if you have totaled up the number of hours of frustration, the number of service calls people have to place. It's a very expensive problem. I don't see it going away.

I think it is going to increase and increase until we get some suicides or something.

MR. KOEHLER: I'll open it up to the panel. Is there any additional evidence or are there other studies done like Roger has done?

MR. WOOD: Not so much a study, but anecdotal in looking towards a previous question where we were talking about business. That moves in the same direction as far as business is concerned. You are going to have more down time. You are going to have computers that just aren't functioning properly. You are going to have situations where just running a program, to keep that clean, instead of having to call in expensive technicians, small companies have to call someone in to fix it, that's significant productivity loss, expense, et cetera.

It's just getting to the point where it is unacceptable.

MR. KOEHLER: Let's turn to an issue that we have heard a bit about in the press as well as today, and that's hijacker browsers. Does anyone want to address that and what kind of concerns that creates for consumers?

MR. GORDON: I can specifically talk about some of the security issues around the browser hijackers. It touches upon something that John just mentioned, which is your mom wanting to install AOL 9 and being told go run one of these anti-spyware programs first.

That's really the best case scenario. One of the worse case scenarios is let's go back to the Fall of last year, when the Blaster Worm was running rampant around the world, and everyone is being told go to Windows Update and update your patches and you will be fine.

You were told two things. Number one, update your patches. Number two, update your antivirus software.

And then we started getting calls off the hook to our tech support stating I can't get to Windows Update and I can't get in my DAT file, my signature file, for my antivirus software.

This is where these browser hijackers are coming in, because of the fact that they are redirecting,

they are doing various other malicious things to your PC, either intentionally or not. The fact is they are posing a serious security threat because there are vulnerabilities reported all the time which hackers are taking advantage of, and which spyware companies are taking advantage of.

Blocking the user's ability to go and get their Windows patches, which is just so fundamental to the system itself, it's absolutely detrimental, and it's a serious problem that we have seen a lot of.

When I say that spyware is a top issue for McAfee, it's that issue itself. It's people calling in and saying I can't get your software and I can't get my Windows Updates. That is something that we have been taking steps to help alleviate, but it is still absolutely a problem.

MR. GILROY: Last Thursday I had a client call me up and their browser was hijacked. I would imagine there are people in this room here, I would imagine probably 20 to 30 percent of you have encountered this.

Sometimes it is just as easy as resetting the home page. Sometimes you have to really start scratching your head and trying every single different angle to try to overcome it.

I think it's a serious problem and it costs

people a lot of time and frustration. My specific situation where I respond to people on the radio and I respond to people in the newspaper, it's more and more. It's almost a standard call now.

MR. KOEHLER: Can we step back a little bit and address, without getting too technical, the mechanics of a browser hijacking and how it affects computer settings?

MR. WOOD: There are several ways that can happen. An application can install itself and actually lock your browser, change its settings, et cetera. There is also another exploit where they can add an entry to your host file, much like the old block list that used to be on the Internet before a lot of the applications that are available today, where it will not allow you to go to that site.

We have seen entries that don't allow people to go to McAfee, don't allow people to go to our sites, Pest Patrol sites, virus companies, et cetera.

It is a huge problem.

MR. KOEHLER: The issue of security risks was just mentioned. What sort of security risks does the installation and operation of spyware impose?

MR. THOMPSON: One risk is that if you think about the peer to peer form of adware/spyware, every one that comes out now drops itself, it looks for the shared

folders and drops itself into those shared folders with enticing file names in the hope that somebody will actually come looking for them, Britney Spears, something or other, LaToya. Whatever sounds enticing, and they hope they will be pulled into other people's machines that way.

The really worrisome respect, there are two. One is that the bad guys you can bet are probing, constantly looking for a way to actually hijack the update mechanism, the trickler, as we call it. If they can find a way to hijack a trickler, then they can instantly insert themselves into these massive networks.

I was going to say something else, but I forgot. I must have a virus.

MR. GORDON: I can chime in on that one. Touching on what Roger said, absolutely. What we see is there is a sharing of technology everywhere. You have the hackers learning from the spammers. The spammers learning from the virus writers. Everything is out there, and everything is out there for the spyware writers to take advantage of, for the hackers to take advantage of, and so on and so forth.

Talking about propagation techniques, in many of the new worms we have been tracking, absolutely, many of them do look for that shared folder as part of the

peer to peer network and try to drop into that as means to spread across the Internet faster. E-mail is still by far the number one means for propagation among worms today.

The thing is a lot of the threats that you hear about is just really the tip of the iceberg for the threats that we actually see. There are other things out there that never hit the press.

Trojans, for example, that will go out and take a page from the peer to peers themselves and set up their own peer to peer network on a person's system. Setting up this network, it can actually then spoof legitimate peer to peer networks and take advantage of their users, and spread things like keyloggers across the Internet, dropping onto a person's system and grabbing the keys and sending them back to some remote location.

I don't want to draw any sort of clear lines between the adware, spyware and all those things, because of the fact that all these technologies are being shared, and there are a threat across the board.

MR. THOMPSON: That is exactly right. That is part of what I was going to say, too. Thanks.

There are these things called Bot farms, as in robot farms. Some people call them Bot armies. If they get up against some website in a malicious service, it

becomes an army. Prior to that, they are a Bot farm. Nobody really knows who is doing it. Massive Bot farms, many, many massive Bot farms build up around the world.

The guys who are taking over these farms, they have turf wars trying to take over each other's farms. They fight over each other's farms and try to build their farms bigger. Nobody knows really who is doing it. It's very routine to log into one of these Bot farm controllers and find there is 1,000 or 2,000 nodes locked in at that very moment.

All of these computers are computers that are a bit of back doored with the worse kind of spyware. There is no doubt there are keyloggers involved there.

The part that scares me the most is if I was a really bad guy, if I was organized crime, I would take a long term view. I would write the good ad that's useful to people and I would partner with somebody who is already pushing this stuff out legitimately, and I wouldn't do anything for three months. I would just get out there and behave and be like a legitimate ad, and then I'd start doing whatever it is I wanted to do.

MR. KOEHLER: What would that be?

MR. THOMPSON: Steal credit cards. You could farm the credit cards. You could just take a few at a time and no one would know. No one would know how it was

coming in.

MR. KOEHLER: Has the panel seen any instances of other potential risks of a Bot farm or exploiting a security issue whether it's using a computer to send out spam or to mount a service attack?

MR. GILROY: I guess it would depend on how wide ranging you want to define "spyware." I had a client's machine and I looked on the hard drive, and there was a hidden file on there with three gigabytes of information on it. It was just sitting there doing nothing. He was obviously using it to store, and the person didn't know it.

This is the upsetting factor. What is that computer doing, is somebody storing bad software on it and you don't even know about it. This is really frustrating.

Spyware on your machine and your machine could appear to work properly and you are not even aware of what's going on in the background.

I gave a talk with a person from True Secure, and he asked the room how many people know that their machines have been hacked. No one held up their hand. Obviously, something was going on that people don't realize. I think it's even more scary when you don't know what is going on.

I think spyware can be more pernicious than some viruses because you may not know what is going on in the background. That was storing a lot of information. I was surprised to find that. It was interesting.

MR. KOEHLER: Does anyone else on the panel have any anecdotes or experience regarding these uses for spyware, whether it's initial or ultimate uses?

MR. GORDON: Again, like John says, I know we don't have any definition yet for what we call traditional spyware. However, if we just want to talk about malware, these Bot farms are the reason for a lot of the wars that we see lately between the Netskys and the Bagels and the MyDooms of the world.

An interesting story that I saw if you can see sort of groups of Chinese hackers that have their own sort of Bot farms undercutting some Eastern European Bot farm managers, if you want to call them, because they are willing to do various jobs in terms of sending out spam for less than the Eastern Europeans will do.

You see ads on the Web for a company that will state I have 250,000 hijacked machines in the U.S. with broadband access and I will send out your spam for X amount of money per e-mail. That's common.

MR. THOMPSON: That absolutely happens.

MR. KOEHLER: Roger, you mentioned something

earlier regarding hijacking updates. I will open this to the panel. Has there been any issues regarding particular security risks dealing with auto update features?

MR. THOMPSON: I think it's early days on that yet. I don't think it's happened. I know the bad guys are probing, they are looking for ways. We are trusting that these guys have done their homework and have done their security properly as opposed to just going for the best possible quickest update they can.

MR. GORDON: It's all about propagation. Why do virus writers use e-mail? They use e-mail because everyone uses e-mail and it's the most efficient way to propagate a virus or worm across the Internet.

Have we seen spyware update components being exploited? No, not yet, but as we hear numbers like 100 million installations of adware or other companies claiming 50 million, 100 million. As those numbers increase, I guarantee that the virus writers of the world are going to take notice.

As peer to peer applications took off, we started to see all of the virus writers now just throwing in additional propagation tactic within their new malware, like dropping a file like Britney Spears into the shared folder.

While we haven't seen it yet, it is going to happen as these things become just more widely adopted. "Adopted" is a loose term. As they become more widely adopted across the Internet.

MR. KOEHLER: What has been the panel's experience in terms of spyware, whether or not it can exploit a consumer's security settings and interacting with the security settings? Is there activity between spyware and that?

MR. THOMPSON: Are you asking have we seen that happen?

MR. KOEHLER: Initially, have you seen it happen, and if not, is there the risk of that happening.

MR. THOMPSON: The more malicious forms of spyware, absolutely; yes. That's what they do. The common adware doesn't really do that. They are trying to be legitimate applications.

MR. KOEHLER: Is there a possibility that spyware can evade security settings and security applications at this point?

MR. THOMPSON: Ask your question again. I'm not quite sure what you are getting at.

MR. KOEHLER: In the experience of the panel, has there been any instances where a particular bit of software that we would label as spyware, that it has the

ability to evade --

MR. THOMPSON: Absolutely. That's another trend that we are seeing. If you went back two or three years ago when the thing was first starting, they tried simply to hide and do everything on the back channel, but we are seeing more and more, they are making themselves harder to get out. They will have two programs in memory that protect each other and when they leave one, the other one will re-load it. If you delete the registry keys, they will re-load it.

Not all. That's getting close to the line between being overtly bad and possibly bad. It's a trend that we are seeing, definitely. At Lavasoft, you are probably seeing the same thing.

MR. WOOD: Definitely. There are other issues, too, especially with NTFS systems with alternate data streams. We are actually looking into with our next bill we are going to have that available where it can be scanned. You can attach a file of any size to any other file folder, directory. It doesn't really matter. You won't be able to see that application.

In fact, you could have nested alternate data streams and not be able to see them unless you have those special browsers or technology to look for it.

MR. THOMPSON: That's not doing anything

overtly bad either, it's just taking advantage of an operating system.

MR. WOOD: Exactly.

MR. KOEHLER: Regarding those risks, are the security risks different for consumers then businesses and why, if so?

MR. GORDON: I don't know if the security risks themselves would be different. It's just the awareness of those risks within the consumer landscape is almost non-existent. Or as in many enterprises, at least they will have some sort of IT department that in part at least is dedicated to security on those user systems and will try to do whatever possible to make sure those settings are high enough that they are not being exploited by spyware.

MR. WOOD: I'd say as far as businesses were concerned, the most important asset a company has is its information. It doesn't really make much difference what that information is, even if it's something as minor as where Johnny surfed today, to actual keyloggers being on their system and collecting proprietary information. It is still important for businesses to want to protect that, to keep that information private.

Any transmission of the information really constitutes a security hole.

MR. KOEHLER: Thank you. Let's assume for the sake of argument that we have spyware on our system, by any definition we want to use. In terms of removal, and compared to most software, is spyware any more difficult to remove than other software and why?

MR. THOMPSON: Absolutely. The reason is if you have a virus on your system, it's usually one thing. If you have a worm on your system, it's usually one thing. It might have a bunch of files, but it's the same thing every time. It might be a single registry key.

With the adware apps, they might drop 4,000 files -- a single installation might drop 4,000 files on your system and making 2,000 registry changes. What that means is it's very difficult for other software to go and just drag that out and take that out by the roots if they provide an uninstaller, you just run the uninstaller and get rid of it that way. Sometimes they don't provide an uninstaller, and if you try to do it automatically over a network, that's real hard. They are much harder. That is not counting the ones that actually defend themselves.

MR. WOOD: I definitely concur with that.

MR. GILROY: From a consumer's perspective, this is what a typical consumer is going to do. He is going to go to Google and type in "spyware detector" and he gets 40,000 hits. I did that yesterday. What a lot

of consumers don't realize is that many of these products can be in fact spyware.

The Center for Democracy and Technology, I think they have a lawsuit now. They are suing a company that purports to be an anti-spyware product and actually it comes in and it blocks a lot of things from happening. I think it even blocks your antivirus from updating and it allows their code to come in.

The typical consumer solution of going to Google and typing in the answer and coming up with something can be deceptive in and of itself. There are no standards for spyware detecting utilities out there.

MR. KOEHLER: What are some of the problems particularly with the software manufacturers on the panel, what kind of problems do you face in determining what sorts of -- Austin, welcome.

MR. HILL: Sorry.

MR. KOEHLER: Austin, we were just discussing some spyware removal problems. Feel free to jump in, if you wish. As he is getting set up, if anyone else wishes to address the specific kind of removal problems and issues that the software manufacturers are addressing.

MR. THOMPSON: Again, it's just the sheer volume of changes they make to a disk. If you think about a Trojan, it probably drops itself in one or two

places and maybe affects one run key or something in the registry, that's three things you have to remove. An average pest will drop 4,000 files and maybe make 2,000 to 3,000 registry changes. That is hard to reverse.

MR. HILL: I guess taking a different side of it, the pure technical issue of the problem of removing it, one of the things we see, we work in the call centers of probably around 10 million consumer ISPs. We represent the security expertise for those consumer ISPs.

One of the problems we are seeing is that consumers don't understand if they have adware, malware, spyware, they don't know. The people who are obviously having the problems, one of the first people are ISPs. They are having a six minute on average call with an ISP, if it's billing related or any other problem. When it starts to become technical and a security issue has to be troubleshooted by the ISPs, that now is on average 25 minutes for a support call.

The difference in cost of that is somewhere around $15. When you have someone pay for a $20 to $40 account a single call to the customer service agent, it wipes out an ISP's entire margin. They are really bearing the brunt of this because consumers don't understand and the ISPs are now having to take responsibility for helping them figure out why their

computer isn't acting like it should.

MR. KOEHLER: Austin, perhaps you can address a question that we were working with earlier, and give a perspective given your work with ISPs.

What is the trend line that you see regarding complaints about spyware and spyware related issues?

MR. HILL: It's very hard to break it out for spyware specifically. We tend to track all security related incidents. On average, for every million customers that an ISP customer has, there are obviously some savings and it depends on what they do, but on average, they run 1,500 to 2,000 security related calls into an ISP's call center every week.

The trend or the experience tends to be -- this is why I kind of talk about it more as malware than spyware because it's my Internet or my PC is doing something unexpected, whether it's sending out e-mails, they are getting the wrong search page every time I kick up my browser, all of those create an experience where they go to the ISP, a lot of times they are angry and frustrated. They feel the ISP should do something about it. Other times, we have seen, not a huge trend, but some people moving away from broadband and going back to dial up. They feel it is just too much of a hassle, it makes them too much of a threat. They say I'm paying

almost double, why should I stay on broadband when it makes my life more miserable. It's not worth the faster speed.

Then you see churn rates. Churn rates or cancellations among ISPs directly related to -- call it malware. It's too slow, I'm getting all these pop ups, I have a worm, all of the various things that consumers find a security issue tends to run around 1.5 percent over a 12 month period. Those are very expensive customers to lose when you are having customer acquisition costs being very, very high.

For the ISP's losses directly, they are in the millions. An average sized ISP is directly being hit with support costs, cancellations, that is affecting them.

MR. KOEHLER: Thank you. Before we move to questions from the audience, I'd like to give the panel an opportunity, as we look at the current trends, if we could look at the future trends a little bit, what each panelist seems to think that the biggest security risk or functionality risk out there that we are going to face near term is going to be.

Michael, would you like to start off?

MR. WOOD: The biggest trend that I think we see is just that they are going to increase in number.

No matter what we do to mitigate it, to get a hold of it, remove it, et cetera, they are just coming out with different new variance, et cetera, trying to stay ahead of us. They are not really spending a lot of time with their applications and really causing a lot of trouble.

I really just see at this point that the situation, the behaviors, et cetera, we need to get a hold of them so we have some remedy for it.

MR. THOMPSON: I have actually been in the antivirus industry for a long time. It actually can be tracked to various ages. I'm absolutely firmly convinced that we are in the fourth age of malicious code and the adware/spyware area is one of those streams.

The interesting thing about regular viruses is they are normally written by one or two guys and they eventually grow up and get a job or get a girlfriend or get a life and they stop. The adware stuff is written by a company with a whole company behind it. It's a profit motive. So, guess when they are going to stop. They are just going to keep pushing the envelope.

I'm firmly convinced that we need some legislation. I don't think legislation will stop it because people will work around it. We need to have some legislation, in my opinion, that draws some lines and makes it a bit clearer we are not going to overstep those

bounds.

MR. HILL: I think one of the challenges, the greatest ones is the complexity that consumers are being burdened with, having to understand and become experts, having to go and research the solutions, track their antivirus, keep track am I up to date on this, do I have my pop up blockers, do I have this, do I have that.

If it were this difficult to drive a car, we wouldn't have any oil crisis because no one would drive.

Unfortunately, the same burden isn't put on the computing industry to make it a safe, simple, pleasant experience to track with technology. That is costing the industry a huge amount of money.

I think what we are going to see is a shift. I don't think it's going to come from liability, unfortunately, there is not a lot of liability issues that are associated with software, but I do think that the industry is starting to get some sort of idea on the costs and the burden to have consumers stop having a pleasant experience with technology, there are consequences to that, par financial numbers.

I think the responsibility needs to be more to the providers of the technology to embed and secure consumers, if they still want to enjoy that good relationship with them.

MR. GORDON: Just building on something that Roger was saying. Yes, a lot of the virus writers of the sort of mid-1990s are growing up and getting lives now, but there is a core group of them that do have the cars, the mortgages, and they need to pay for these things. They are using their talents to actually create what we have been sort of referring to as "worms for profit."

A lot of malware and a lot of viruses, worms, et cetera, have this new sort of motivation behind them. It is not look what I did, I'm so cool, I'm going to show off to my friends that I just made this cool virus that drops a little bunny rabbit on your computer. It's not really about that any more. We don't see much of that.

What we see a lot of is these worms that are trying to take advantage of an user system, to open the back door on the user system to send out spam.

If you look at the MyMail stream of viruses, that actually was the first really good example of a fishing scam being combined with an Internet worm that could get your paypal information and other credit card information and hijack that, by using the worm's propagation techniques.

I think in general where McAfee really sees this going is that convergence of technologies and that convergence of threats.

We are already seeing Trojans that are dropping keyloggers on systems, and I think as more and better technologies are developed to combat spyware, they are going to have to take a page from the virus writers of the world and figure out what are the ways around these technologies, what are the ways that I can better propagate spyware, because it is a business. That's the key difference. People are making money.

Whenever people are making money, they are going to do whatever they can. They are going to adopt whatever technologies they need to adopt in order to make it more sophisticated so that it will propagate and it will affect people around the world.

MR. GILROY: David wanted to know about security concerns for consumers. I think consumers are going to take it to the chin for the next couple of years, and the computer technicians are going to be having a great time. They are going to be making a lot of money repairing these troublesome problems.

In fact, I'm starting to tell people if they are having a hard time with their hard drive, they should look for spyware.

MS. CUSHMAN: You asked about trends, to put a hopeful note on John's comments. We are encouraged by some recent efforts of consumer education that Dell has

undertaken. We do feel like we are answering consumers' questions and helping them get the full benefit of their systems back.

This workshop and other industry efforts, consumer education, hopefully can allow consumers to have control over their systems.

MR. KOEHLER: Great. Thank you. We will move to some questions from the audience now.

The first one is how does certain spyware defend itself to events or inhibit removal?

MR. THOMPSON: The very worse kind are the ones that actively put themselves back in the registry as quickly as you remove them, and then the ones that have a partner, so there are two programs that help each other in memory and they defend each other. If you kill one of the processes, the other one immediately re-loads it.

That's about the worse. Mostly, they just change their load frequently, the set of definitions used to remove some of the adware a month ago may no longer be appropriate. It might be a completely different load, they might put things in completely different places.

Another thing that they do that makes it tricky is you can usually install them all with a single click. There is usually one place where you can say okay, I can read all these different end user license agreements or I

can just click here to say that I've read them all, and guess what most people do, so you can get all this stuff with a single click.

If they provide an uninstaller, it generally means if you have five programs with a single click, you either have to go and uninstall all five, if you just uninstall the main one that you knew you were getting without realizing you got these other things as well, they still have you. They are still running the tricklers. Give it a week, and it will all be back.

MR. GORDON: It's just interesting to point out quickly that type of sort of self defending technology, multiple processes running at the same time, if one goes down, the other one kicks in and they help each other out, that's something that has been around in the virus world for a while now.

When we say that technologies are being shared, the spyware people are going, hey, wait a minute, why don't we grab that self defending technology that ABC virus used and see if we can help prevent the removal of our application from systems.

MR. WOOD: Another part that makes it even more difficult with the two program example is that they will more often than not use random file names, random paths, file names that you wouldn't even recognize, if you find

one and remove it, it doesn't remove the other one and reinstalls, it's going to reinstall with a new name. You can't really track the names. It's all random.

MR. KOEHLER: This actually raises another issue, in terms of the registry. Is it a good idea for the consumer to be tinkering with the registry, to make changes to spyware? John, maybe you can address that.

MR. GILROY: I would probably avoid the typical end user diving into the registry. There are utilities that you can buy that will clean up your registry.

You buy a computer and there are 300 different tools. You have anti-spyware utility, a registry cleaner.

I don't think a typical consumer should dive into the registry unless he uses a program that is designed to do that.

I'm sure that some of the people on the panel have seen some of these nasty tricks. I've seen some code in registries that is fascinating. These guys spend so much time writing this code. They must not have a life.

MR. THOMPSON: Either that or they are making a buck.

MR. KOEHLER: What about the anti-spyware programs, is there any experience in terms of things

being either removed from the registry and elsewhere, a consumer using those programs and moving things about they shouldn't be?

MR. WOOD: Quite often, somebody who is inexperienced may actually remove something that is legitimate, is important for the operating system. You can't really tell. Sometimes they will name it as something that is legitimate, so it's hard to find. If they remove the wrong thing, they could ultimately have to end up reinstalling the operating system.

It's one of those things that you really don't want to have anything to do with unless you really know what you are doing.

MR. THOMPSON: There is another nasty trick that they use, and I neglected to mention it before, and that is they insert themselves in what is called the LSP chain, and effectively what that means is they burrow their way into your TCP stack and if anybody doesn't know what that means, they hook themselves into your Internet connection, and it becomes a chain.

Whenever something goes to the Internet, it goes through all the programs that are hooked into this chain and they all have a little look at it.

The bad part about that is you can't just delete the program without re-patching the chain

properly, or if you do, you lose your Internet connection. That spoils people's day.

MR. HILL: I think the comment about should consumers get involved, consumers don't want to. I don't know anyone who has a burning desire on average to go look inside their registry. It's actually boring, if you have ever tried it.

Consumers are being pushed or burdened to have to get to know this stuff, and that's the unfortunate thing. They are the ones who are saying okay, my Internet isn't working, something is wrong, so either they are calling the little technician or a friend of a friend or so and so's kid to come over and try to diagnose it. It leads to a high level of frustration.

There is a lot of debate over is it adware, is it malware. They agree to install it. I can't buy into that because by and large, consumers are being faced with an experience that was not the experience they signed up for. I think that's the critical test on whether or not something is malware or not, did a consumer say yes, I want my web page to now go to this other site, unintentionally or not, that's a very easy thing to do.

You go and change your book mark, you go change your starter page. When it's happening without them being involved, that's something the consumer is

frustrated about. They shouldn't be burdened with having to figure out how to switch that back, especially as we've heard, when the program makes it very, very difficult for them to do.

QUESTION: Can we ask questions?

MR. KOEHLER: You can do cards and send it forward and we can ask them as time permits.

Here's a question for the panel, and this might address the aggregate numbers issue. Aren't many spyware programs downloaded from pornographic sites and other places that repeated users might not admit to visit, and do you think some consumers might be lying when they say "I don't know where I got this?"

(Laughter.)

MR. GORDON: I have a good story about this one. One of our senior virus researchers was recently talking to his son's elementary school's class. After he gives a little talk about what his job is and what he does, one of the fourth graders puts up his hand and says, mommy and daddy found a virus on our computer and then they had a big fight about the phone bill.

(Laughter.)

MR. GORDON: Just dialers in particular, we have detected over four million of these things in the last eight months. That's the kind of thing where we get

the call, I have a $3,000 phone bill, I've never gone to a pornographic site in my life, and yet I'm being served with all these things.

Yes, people don't want to admit to it, and that's fine, and that's why you have to get the technologies out there that will prevent those things from getting on the system.

That said, these are not limited to pornographic sites. The interesting thing was the last time I was in D.C. talking about spyware and waiting to get into some press office, and the security guard saw I was from McAfee and said, my son, he goes to all these sites, he goes to all these gaming sites, and we keep on getting all this adware and spyware on the system. His son may be going to pornographic sites as well, but the fact is a lot of these sites where kids are going, in order to look at some what are all the cheat codes for the latest X-Box game or any other thing like that, a lot of these things are hosting spyware and adware in dialers.

It's the type of thing where a kid could be legitimately going to try to find the codes for Grand Theft Auto and the next thing you know, his Internet connection has been hijacked and they are paying $100 a minute and the parents don't understand why the phone

bill is so high.

MR. THOMPSON: That's very true. I'm pretty sure that the most egregious forms of spyware generally come from either a website of ill repute. The adware comes from people doing something much more legitimate.

MR. HILL: I actually got hit here with my own PC. I do all the tools. I run the tools. We have software. I have all my PCs perfected. I taught my girlfriend not to install things. Don't go to web sites that you can't trust.

Her cousin was visiting over Christmas, and it was during a two day window when before signature files had been updated, and it was combination malware, spyware, reset all the browser settings, the PC is melting down. I'm updating all my batch files.

I end up just wiping the system and having to reinstall it. I've been working with computers since I was eight, you know. I'm an expert. Even with all the tools sitting right there, I still ended up having to wipe out the computer and just reloading everything. It took me around five days, if you have ever rebuilt your computer. Once you get everything back installed, locate all your serial numbers.

That is what consumers are being faced with. Where do they get it? I don't know what he was doing on

our computer. The fact of the matter is even as a computer owner, I can't always protect -- computers are so shared today, it's impossible for me to ensure that everyone that is using it is going to have my common sense. That's why we need more technological solutions.

MR. WOOD: Exactly. I concur with that.

MR. KOEHLER: This addresses the issue of adware that people may want on the computer. The first panel distinguished spyware from adware on the basis that adware is clearly labeled, the consumer knows about it and can easily uninstall it. Does adware defined that way also cause the problems you discussed, like slowing down the computer or making access harder?

MR. THOMPSON: Absolutely. I'm not saying that adware is necessarily a bad thing, but people have to understand that they are paying a price for it.

MS. CUSHMAN: I would second that. I think along the lines that I have discussed already, I think consumer education about the ramifications of what you load on your system is really important.

Certainly, consumers should be able to make a choice and then take off anything they don't want or don't need any longer. Hopefully, consumer education can be an answer here.

MR. HILL: There is also a build up over time

because you install that one utility that is very useful at the time you started using it, and then you say, okay, I'm getting a few more ads or a few more pop ups. All right, so you accept it. It slowly adds on. You have this other utility you install, and it starts to build up.

Now all of a sudden a huge amount of your resources, a huge amount of your screen space, a huge amount of your experience, it becomes very gradual. What that leads to is something is wrong with my computer, it's not working the way it should, or calling the ISP saying your Internet is very slow. It's not my Internet that's slow, you know, we can do all the tests. We work in call centers, and this is what ISPs are bombarded with. Consumers just say well, something is wrong, I'm paying you $40 a month and I'm getting pop ups and it's slow.

To walk through that diagnosis, the customer service agents are now 20 minutes trying to go through which program did you install, which one did you want, which one should be uninstall.

Without new tools or new methods to give consumers more control, and also to assist the people who are on the front lines. It's one of the kind of dirty secrets of the security industry that I have begun to

realize, when this happens, companies are very defensive. I need to protect my network. ISPs really are in the trenches. Their call center agents in ISPs bear the brunt of almost every major outbreak, malware, adware, more than anyone else, and to date, their only response has been go down to Best Buy and pick up some software.

It doesn't really help. When CNN runs a big thing on spyware, guaranteed, next day, our call center agents start getting calls where users say how do I know if I have that.

Even if they are running up to date software, they still make a call to ask the ISP. There is education needed. There are new tools needed. The paradigm really has to change so that people feel protected and don't feel as threatened on line.

MR. WOOD: Just to build on that, think of your computer at home. You might have 30 or 40 processes running. You open up programs and start to use them. You notice your computer slows down. Now imagine if you had 600 to 800 running.

MR. KOEHLER: That certainly sums it up. I think with that, I will thank each of our panelists for sharing their experiences and expertise.

It is quite a wide spectrum that we are looking at, whether it's a small system slow down or the size

that you are describing to the other extreme of Bot armies and the potential they hold.

Although these types of threats are difficult to quantify with precision, it's fairly abundantly clear that the amount of spyware that is out there as well as the consumer concerns about it is growing rapidly and deserves close attention.

Thank you very much.

(Applause.)

(A brief recess was taken.)

MR. PAHL: We will start our next panel now. Our next panel will be moderated by Dean Forbes, who is an attorney in our Division of Advertising Practices. If I could ask everyone to please sit down so we can begin the panel.

Thank you. The moderator of our next panel is Dean Forbes, who is an attorney in our Division of Advertising Practices here at the Federal Trade Commission. I would like to thank Dean and the rest of the members of our privacy panel, welcome to the FTC, and I will ask him to begin.

MR. FORBES: Thank you, Tom.

I'd like to introduce our panelists today. To my immediate left is Ray Everett-Church. Ray currently serves as TurnTide's Chief Privacy Officer and has served

as CPO and Senior Vice President of Consulting for ePrivacy Group. Prior to that, Ray served as the world's first corporate CPO. He is the co-founder of CAUCE and is the co-author of Internet Privacy for Dummies.

To his left is Evan Hendricks. Since 1991, Evan has served as the editor and publisher of Privacy Times, a bi-weekly newsletter in Washington that reports on privacy and Freedom of Information law. He serves as a privacy consultant to Federal, state and business organizations, including the Social Security Administration and the U.S. Postal Service. Evan is the author of three books, including Your Rights to Privacy.

To his left is Chris Jay Hoofnagle. Chris is the Associate Director of the Electronic Privacy Information Center or EPIC. Chris has testified before Congress on privacy, identity theft, and related issues, and among other things, Chris' recent work has focused on the privacy implications of the merging technologies including invasive advertising and digital rights management.

To his left is Jim Koenig. Jim is the co-leader of PricewaterhouseCoopers' privacy practice. Jim's business technology and legal background include work with QVC/ Comcast. He served as the chief legal development officer for ePrivacy Group where at the time

he was the expert in FTC's cases against Eli Lilly and Guess.

Jim currently serves on the Board of the International Association of Privacy Professionals and is its general counsel.

Last but not least is Ron Plesser. Ron is a partner at the law firm of Piper Rudnick, where he serves as the chair of the firm's electronic commerce and privacy practice group. His clients include trade associations and individual companies that he has represented before the U.S. Congress, Federal agencies, and all Federal and state courts.

I wanted to start out by summarizing a bit of what we have heard. I want to encourage our panelists to speak as closely to the microphones as possible when answering questions.

What we are going to do is follow a similar format of what we have done already, which is basically to start out with questions, and then have panelists respond directly.

We are working from the definition, the working definition, of "spyware," that we have put into the Federal Register Notice that announced this workshop, which was expounded upon by this morning's panel, which addressed definition and other concerns.

Just to sum up, spyware software is downloaded to a PC that aids in gathering information about consumers or organizations, and that may send such information to another entity without their knowledge or consent, or it may assert control over a computer also without knowledge or consent.

We heard this morning from the panel, I think there was some agreement on the definition. I think there was some consensus there. I also heard from a number of panelists, including Ari Schwartz from CDT that a lot of the issues do revolve around the issue of privacy.

We can talk about different technological concerns, whether they are the cookies that were an issue in the past, but maybe the focus isn't the technology, but really is -- while there are technological security and functionality implications of spyware, a lot of it does turn on this issue of privacy.

Turning right to questions, does spyware collect and misuse personally identifiable information in ways that violate consumers' privacy? Consumers may not understand that the explicit recognition of risks and rewards that are related to spyware and the tradeoff they engage in.

My first question is going to be to Chris, Evan

and Ray. What is privacy risk as it relates to spyware?

MR. HOOFNAGLE: There's a quote in this morning's Washington Post saying that spyware may be used for more benign purposes, including consumer tracking. It is exactly that type of practice that we think is highly privacy invasive, and outside the expectations of consumers.

We have a wealth of data at EPIC.org/privacy/survey, that discusses individuals' expectations when they go on line. These are polls done by independent groups, Annenberg, groups including ASNE, the American Society of Newspaper Editors, that show that a substantial majority of Americans do not want to be followed on line, and they think it is an invasion of privacy to be tracked on line.

There is also increasing resistance to consumer tracking, even in the aggregate, when personal information is not even involved.

For instance, if you look at yesterday's Washington Post, there is an article discussing consumers who were unwilling to even share their zip code because they do not want to share any information that feeds into the marketing machine.

Another recent survey released by Yankolovich Partners last week cited that 61 percent of Americans

think that there actually needs to be increased regulations to deal with the invasiveness of advertising. 65 percent reported that they thought advertising was out of control.

The privacy risks here are wide. They include actually stealing personal information, monitoring actual communications, but as for individuals, as for members of the public, mere tracking of on line activity is privacy invasive. It's not benign.

A consumer protection advocate would not align his or her values in such a way that consumer tracking on line would be a benign practice.

MR. HENDRICKS: It's interesting in covering both privacy and Freedom of Information Act, some of the most interesting discussions on privacy by the Supreme Court are in the FOIA rulings. The Reporters Committee of the Supreme Court said that privacy begins with the right of the individual to control information about themselves.

In this recent case involving the suicide photos of Vince Foster, the lawyer advocating disclosure said that's the only definition of "privacy," and this doesn't involve that, so privacy doesn't protect the information. The Supreme Court said no, that's one definition, but "privacy" is a very broad subject, and

the solitude and dignity of people and survivors of suicide victims also is a privacy issue. They left the door open that they will go on and identify other privacy issues as they come along.

That means that the privacy risks that arise from spyware are also very broad. They are the capturing of data, without people's knowledge and consent, and putting it out of their control.

Identity thieves are very ingenious, and industrious, and those that get arrested talk to each other in prison, which we now know is happening, so they can talk shop and find new ways of doing it.

They probably already are jumping on this sort of technology to take advantage of it.

In the last panel, you heard Austin Hill talk about the intrusion into your experience and disrupting that experience. That also is a privacy issue.

Chris alluded to the chilling of communication. If you know you are being monitored, and if you don't believe me, ask Alexander Solsynitsan. If you know you are being monitored, it can affect how you carry on, how you use a communication system or do not use one.

Those are some of the risks. The final risk is to the system itself. I think Austin Hill also referred to this. This is causing an unpleasant experience. If

the surveillance and the hassle involved is not worth using the medium itself, then you risk people dropping out of the system. We saw this earlier with things like the 900 phone number which started out with great promise and they got so tired to fraud and pornography, it isn't even in existence any more.

The ultimate risk is the risk of losing a very valuable system or denigrating its usefulness.

MR. EVERETT-CHURCH: Thank you. I won't repeat Evan and Chris' excellent summaries there, I just want to highlight a couple of elements.

In previous panels, we have heard folks saying that the kind of information being gathered by many of these spyware and adware applications is often anonymous or in aggregate, and if it is truly anonymous or in aggregate, the privacy risks can be to some extent mitigated, but my concern is that many of these applications engage in deceptive practices to be installed or to operate in a fashion that makes them difficult to understand they are operating, to understand they have been installed, and difficult to uninstall.

This level of behavior and deceptive practices gives me some question as to how much confidence I wish to place in their claims about this being very minimally intrusive, anonymous or aggregated information,

considering you have applications that themselves can be modified and changed and could become a new security threat as we heard from folks on the last panel talking about as the software itself could potentially be hijacked, have its own security risks, that open up consumers' computers to new risks.

I also want to say there was an excellent comment filed. I mentioned it briefly in my comments. There was an excellent comment filed by an organization that develops freeware and shareware. They raised some interesting concerns about the perception from consumers that other freeware or shareware may contain suspicious software, may contain spyware and adware, and that having a negative impact on distribution and deployment of new technologies and new useful software applications.

The spill over effects of consumer fear, of consumer uncertainty and suspicion goes far beyond this particular narrow set of concerns.

MR. FORBES: Thank you. We are talking a bit about risks to consumers in the privacy area. I would like to ask little bit about risk to businesses as well.

Before we do that, I wanted to see if we could get some information on this issue of keystroke logging. One of the things that was mentioned in the last panel and shown a slide by McAfee was that there are different

types and levels of information collection by a spyware, one of which is keystroke logging.

Can you expand upon what is collected and how it is done? Thanks.

MR. EVERETT-CHURCH: Sure. I will admit that I have run into very little evidence of keystroke loggers out there and looking at the statistics shown by McAfee, I suggest there is a fairly low rate out there as a percentage of the overall marketplace, but clearly, there are enough infections with keystroke loggers that merit some concern or warrant some concern.

In my opinion, keystroke loggers are sort of the worse case scenario of privacy invasion. They simply will capture any and everything that you enter into your computer, whether it's your passwords, your personal information that you have registered on a website or financial information that you are entering to engage in a transaction, and all that information gathered in context as well as other more personal information, correspondence, communications with friends and family, all of that information can be gathered, stored and transmitted for any and every potential use.

While the frequency of keystroke logging seems to be fairly low at this point, the risks are tremendously high for those who are dealing with it.

MR. FORBES: Thank you. Are there particular risks to businesses in the privacy area that are different or the same as the risk for consumers?

MR. EVERETT-CHURCH: I'll just take that really quickly. Through my consulting work at ePrivacy Group, I worked with a number of corporations over the years who are not only trying themselves to understand how best to use these technologies, to leverage their marketing activities and what not, but they are also seeing the internal consequences of many of these technologies.

In fact, I was just visiting a client a couple of weeks ago who had to have her PC in her office removed by the IT folks in order to have the hard drive cleaned off because she had so many spyware processes running that she wasn't able to get them all off the system. She tried uninstalling and still had her computer slowed to a crawl.

There was a whole day of productivity lost, not because she was meeting with me, but because she was having her computer rebuilt.

(Laughter.)

MR. EVERETT-CHURCH: She was not the only person in that organization. In fact, some number of months ago, we were contacted by an organization, large firm in the financial services arena, who had deployed

across its entire organization an on line set of training tools and educational software tools, and included in that package, unbeknownst to the IT department, was a spyware/adware application.

Unbeknownst to this financial services company, they had deployed a piece of spyware across their entire corporate network, and including PCs where sensitive consumer financial data was being processed and utilized.

This has some real significant impacts beyond the cost to IT departments in keeping computers running and the cost of networking from increased data flows and what not.

There is risk to consumer data in the possession of these companies.

MR. PLESSER: The risk to business I think is it really goes back to the key word "trust" and consumer confidence at several levels. First of all, if a consumer does not have confidence to give a zip code on line, then that's going to impact the legitimate companies and users who need to collect information. It creates almost what sounds like a Wild West atmosphere out on the net. We have heard that before, but perhaps it is here again.

I think particularly following the definition of the FTC, you are going to get really unanimous

agreement that the kind of spyware without knowledge of the consumer, without consent, and losing control over the consumer's computer is bad for the consumer, but it is equally bad for the legitimate business who is trying to do business or create a positive experience for the consumer.

I think if we follow that definition, we won't really have any disagreements. I think it's really the same goal, to try to resolve the differences or concerns of spyware, which is the surreptitious collection of information unknown to the consumer.

The problem comes in, of course, with as you move away from that definition, there are legitimate applications where information may be taken from somebody's computer and used to calculate it at a distant site. That is done by the person you contracted with, and if that's done with knowledge, we think that would not fit in with the definition of the FTC, but the concern, for example, that several of us have with some of the pending legislation, particularly in Congress and in Utah, that those requirements expanded far beyond the lack of knowledge, consent, and control issues to try to regulate generally software, and I think that is where the problem has developed.

On the privacy issues, the way you defined it,

Dean, I think there is unanimous concern that there is risk to both consumers and business.

MR. FORBES: Are some of the risks to businesses -- do some of them include possibly siphoning off trade secrets or other confidential information? Ray mentioned an example with credit card data. Is this a concern for businesses in the area of spyware as it relates to privacy?

MR. KOENIG: Business has had this concern, and often they are better equipped and they have better controls in place to protect themselves than consumers do, but just the same, it is a concern.

As the malware and other harmful software gets more sophisticated, the potential risks to business become that much more pronounced, and so the concern is there, the concern of business being a victim.

Probably what Ron was touching on is the consequence of business who wants to take advantage of the benefits of the new technologies that are there, legitimate uses for potentially tracking and monitoring.

In general, consumers don't want to provide information or to engage in that type of dialogue. Some provide information freely, but very often. Once you have built that trust as a business, once you have built that relationship, both the consumer and the business

want deeper, more meaningful, longer term relationships and value which can be derived from that, monetary, but also from the relationship.

For business, the concerns are both as a victim, but also in being able to move pass the definition. What's left, to make sure as we attack this very harmful problem, what are the appropriate ways for business to be able to utilize this technology for customers and consumers who are willingly and through informed choice deciding to participate, because they want their financial services company or they want their retailer to know their preferences or about them, to be able to provide services.

Once we focus just on the definition, Ron is right, I think we are all pretty close.

MR. PLESSER: Also, I think the risk to businesses is they get blamed. Jules and others will be on later talking about the efforts that ISPs are taking to reduce spyware.

We heard this morning that when there is a problem, who is the first person you call. You call the ISP or you call someone who really is not at fault, but who really has to try to fix the problem and resolve the problem.

It is a problem that hits all of the businesses

working the net, even though they didn't do it, it wasn't their idea, they are not profiting from it, but it's a direct cost for them.

The biggest issue, I think, comes down to consumer trust and the integrity of the system, and this certainly breaks down the integrity of the system.

MR. FORBES: Thanks, Ron. Evan?

MR. HENDRICKS: I think the risk to business, and picking up on Ron's point about consumer trust and confidence, it really strikes at the heart of fear and greed, or in this case, greed and fear, because it is going to impact on customer acquisition and customer detention. There has been a discussion of that in the last panel.

It is also going to be growing liability, even companies -- it's going to be to the point where our companies are doing everything that is reasonable to try to prevent their systems, their employees, or their customers from getting hit by this. You are going to see more and more of that. Of course, the liability on the businesses that are creating this stuff, it's only a matter of time, I think, before they are called to task.

MR. FORBES: Thanks. Thanks, everyone.

The next two questions are pretty similar. What is it that consumers should do to assess and address

the privacy risks that relate to spyware? The follow up question to that is what should businesses do?

I'd like to ask Ron and Chris to weigh in on this first, and then any of the other panelists who wish to as well.

MR. HOOFNAGLE: In our comments we have urged the Commission to continue its advocacy efforts, to encourage individuals to install firewalls, and to use spyware detecting software.

I think what is important to point out, and I think Evan will probably highlight this more, is there is a growing body of recommendations that have been made to consumers in order to protect their privacy.

If you are interested in protecting your privacy, there are perhaps dozens of web pages at the FTC you would have to read to familiarize yourself with the issues, and to actually take the steps you need to take to work on the self regulatory system.

I'm wondering how fair that is. When we think about efficiency or the benefits of the information collection from these various softwares, whether or not we are thinking about the benefits of having greater protections for individuals, and how much efficiency and how much time would be saved by individuals, if they didn't have to become Ph.D.'s in privacy to protect

themselves.

I can throw some technical solutions, some suggestions, we are considering, and I think will be mentioned in later panels for business approaches.

One, I think it's hard to look at this issue without looking at Microsoft. I think it's probably too easy to write to the critical areas of the registry that allow programs to start at boot. Similarly, it's too easy and there is not enough user understanding of the start up folders, which trigger software that you might not want to run.

Serialization is a very important issue, when software is serialized, it makes it easier for people to track you, and if you look at a lot of Windows' programs, including their media player, it is serialized. That creates privacy risks for individuals who want to protect themselves.

Finally, I think it's worth thinking about the relationship of the Internet Explorer browser to the operating system. It seems like a lot of the problems we are talking about today, which are by downloads and by some others, might be limited if we were using browsers that were uncoupled from our operating system.

Let's say you are using Stezilla or Firefox, and that's a conversation we should have.

MR. PLESSER: I'm going to change my answer a little bit, to answer it the way I want to, not necessarily responsive to the question.

I think there needs to be enforcement. If we talk about -- all of the panels are talking about the same thing, but our panel is talking about privacy. I just want to focus on the issue of privacy.

Really now we are talking about theft. We are talking about the theft of information, about somebody, the credit card or address, or we are talking about theft of how they interacted.

It is one thing if this is somebody that the consumer has chosen to deal with, and that's not theft. That's interacting on the site. Now, we are talking about somebody who has come in, switched it up, routed it away.

CDT did a terrific, as everybody is acknowledging it, example document, that I think was just what was needed. You are talking about something at least in my mind which is very serious. I think there is adequate law at the FTC and state AGs and other places on deception and theft of services and other issues where there can be enforcement.

I think these are serious issues. I think the consumer, as pointed out before, is at a real

disadvantage because often they don't know what's going on, they don't know that this has occurred.

I think we really need enforcement. We need government assistance, and we need technological improvements to try to come up with systems that notify the consumer when something is happening, and the ability to de-install.

The last panel, I thought, was great in terms of you de-install one thing and unless you de-install all six, you may not solve the problems.

I think the self help for consumers is going to be somewhat limited here. I think we need enforcement under current law. We need continued technological advancement, industry leadership.

MR. FORBES: How does the regime of notice, choice and control fit into all of that?

MR. HOOFNAGLE: If I may speak about that for a second. The Federal Trade Commission defines substantive privacy rights as notice, choice, access, security and accountability.

I think it's very important that we not allow privacy to be watered down to this idea of notice and choice in this debate or in others.

On the horizon, aside from spyware, I think there are a number of very invasive programs that will

give you notice and will obtain your consent.

In our comments, we discuss this in detail. This is a problem with digital rights management software that secures content, such as music and movies.

The digital rights management software that has been deployed has been extremely privacy invasive. It can track you in many different ways. Professor Mulligan has articulated those risks in a great article.

Those types of programs do give you notice and will obtain consent from the individual.

I think it's important that we set some informative floor, we set some lines in the sand, especially when you look at media companies, media companies that have a monopoly on a certain type of content. You are going to download their media player and you are going to consent to their digital rights management package, if you want to listen to their music or if you want to watch their movies.

The EPIC comments discuss the issue of dealing with privacy on a more normative basis rather than focusing only on spyware.

I think just in summary it's really important that we not boil down privacy to just notice and choice.

There's an Annenberg study that was released last year that said 94 percent of Internet users believed

they should have a right to access all of their personal information on a website. It's those rights of access and security and accountability that are still within consumers' expectations, so we shouldn't start at just notice and consent.

MR. FORBES: Just to sum up, Chris, the normative floor would involve all of the Freedom of Information practice principles?

MR. HOOFNAGLE: You would want -- I think there are some behaviors that you probably want to prohibit flatly, because I think there will be coercive power in this market, especially when it comes to media. If you want to download that movie you really want to see, you will get notice and you will give consent.

Unless there is some floor of protections, banning certain practices, I think fair information practices are a good place to start, but we should think about what these technologies can do and what special protections may be necessary.

MR. KOENIG: I would add to that the thoughts of helping to build common consumer expectations is important. Ron referenced the trust. If you could develop a normative floor to this, I think part of what is important is consumers shouldn't be completely removed from the equation. They should also be informed and able

to make their own informed decisions.

Consequently, the same way that an e-mail under canned spam, there are some common forms of notices there, so consumers can look at e-mail, and while there is always going to be bad actors providing fraudulent notices, common forms of trustworthy notices in time and with consumer experience and education will just be one of the factors in the consumer calculus to determine their trust and comfort level of using the software offered by any particular party.

It's a place to start.

MR. HENDRICKS: I was going to say in terms of to construct the adequate foundation or floor to deal with this issue, you need to go to the Full Monty of fair information practice principles, and those are the eight articulated by the OECD in 1980. I think they are available on EPIC's website and I know they are available on CDT's website.

One of those is data minimization, which is very important here.

Chris says we are in a situation where right now, you do have to have a Ph.D. in privacy to know how to protect yourself, and sometimes that isn't even enough. Not only in this sphere, but in the financial sphere, the medical sphere.

Our national policy default has been to put the burden on the individual at a time when there are all these technologies and data flows swirling around them, and it defaults toward favoring organizational interest.

I think we have to step back and take a very, very strong look at that. The advantage of this workshop, as the FTC has always had all these excellent workshops, is that we are really -- spyware allows you to talk about the two key letters here, S and M. We are talking about S and M. That is surreptitious monitoring.

It comes in the form of spyware. It comes in the form of another letter that has hit the headlines lately, and that is G, Gmail, another form of surreptitious monitoring, and it comes in the form of some of the things Chris was talking about.

In some countries that have gotten out in front of the issue and put the fair information practices into law, some of these things are already illegal. Unfortunately, we have always had a sectorial approach, reacting to the latest problem that arises, kind of like the guy in the parade who holds the shovel following the horse.

I don't think that has proven to be adequate privacy policy any more. I think we need to look at the chain of workshops that we have held and see all the

excellent evidence that has come out of it, and step back and say is it time, have we reached a tipping point where we really need to get out and set a comprehensive policy so that the next spyware subject matter that comes along which needs a workshop, that we are finally going to be out front of it.

MR. PLESSER: If I could jump in. I think Chris' point about normative standards or prohibitions or substantive controls beyond FIP, which are mainly process and procedural, I think there is one area perhaps here, but it's tricky, which is the right to be installed, that any system that doesn't give you the right to be installed is suspect, although as we have heard in earlier panels, for Net Nanny, for child protection, for security issues, you may not always want things to be installed.

Chris, I acknowledge that perhaps there are some areas to talk about, but I think they get very, very tricky and very difficult to generalize when you do put any prohibition in. That one sounds great, as you start to scratch it a little bit, I think you see there are difficulties in putting in that kind of prohibitory rule.

MR. FORBES: Thank you, Ron.

Part of the focus here is on the consequences of harm and the explicit recognition of tradeoffs of

risks and awards. If for example, I download ad supported software, do I understand that I'm also getting something that might be tracking me across the Internet or even after I've gotten off the Internet.

Can Ron or any of the other panelists speak to this issue of clear and conspicuous disclosures, what might they look like, when might they happen.

MR. PLESSER: I don't know that I -- I think a notice is a notice. Some are better than others. I think we have seen -- I don't know that I've seen any in the privacy area, in spyware. I've seen some where the computer will serve you ads that they think will be of interest to you. I think those are usually pretty straightforward. When those ads come in, those alternative ads come in, they have little logos on them, or some of them do, that say this is being served to you by XYZ network, and it's different from where you originally went.

I don't think it's all that difficult, but I think there can be notices that can be workable. Again, I think the DMA is working on this stuff. I think it's important. I think one of the principles that we are working on with the DMA is to make sure these notices are obviously out there before the stuff comes onto the system, that the notice is given prior to installation.

MR. EVERETT-CHURCH: In my experience in researching spyware issues, I have found that notice and the consent process varies widely among various applications. The clarity of the notice in many cases leads quite a bit to be desired, if you look at some of the end user license agreements that you click through.

First off, in many cases, the installation process for a piece of spyware is virtually identical to the installation process and the same screens and the same dialogue boxes that you see when installing plug ins for browsers that are necessary to view particular content.

The Federal Trade Commission website has many documents in Adobe, Acrobat, PDF format. You need a particular plug in to view those. The installation screens for that software are absolutely identical to the installation screens for warning you of the installation of a piece of spyware, and many other multimedia applications.

In most cases, I think consumers have become conditioned and accustomed to seeing those screens as the barrier between where they are now and where they want to be, the content they want to see and view, so they race through those screens, and somewhere in the ad speak and the marketing speak and somewhere in a 10 to 12 page end

user license agreement where the word "pop up" doesn't occur until four pages into the agreement, they don't necessarily have sufficient notice to have made this bargain.

I think there are ways that notice can be given. There are ways to create a more clear relationship in the mind of consumers between this application that they are installing and the pop up ads that are a direct result of this application, because as we noted earlier, on earlier panels, there are instances where the relationship between the ads themselves and the software responsible is only knowable by someone who can paw through the details of a system registry.

MR. FORBES: Thank you. Did any of the panelists want to weigh in on that question?

(No response.)

MR. FORBES: I'd like to move onto what can companies do to assess and address privacy risks as they relate to spyware.

One of the questions that has come up is what are the costs to businesses. For example, in using anti-spyware software, loss of business through redirections or what have you.

Jim and/or Ron, could you please speak to this?

MR. KOENIG: We touched on some of the things

earlier in addition to the costs, the resources, in addition to loss of trust, but there is also consumer confusion.

If there is a pop up when they are on your site that is triggered by something else, they don't necessarily know that's not served by you. Potentially, they are mixing their message with your brand, the company's brand, which is one of the more damaging things. Companies are very concerned about their trust they built with their consumers. Redirection and confusion may be precisely what the spyware is trying to do, to leverage off your goodwill to get someone to act onto another message window and to download other software or to take some other action that with informed and knowledgeable consent, they would not have otherwise have done.

MR. FORBES: How does consumer education play into all of this?

MR. KOENIG: Consumer education is part of what builds trust and confidence, but also I think it focuses on building common expectations.

Ray touched on how those are all over the board. If we could focus on some general commonality, in form and substance, of some of these notices, then consumers in assessing what to do with legitimate

players, there might be a hope there is some expectation.

There certainly is and there will continue to be a lot of fraudulent and bad actors out there, but I think that's the right start.

MR. PLESSER: I think consumer education and consumer notices are very critical, and one of the things that even I find very helpful is a reminder from ISPs and from the services that I use to tell me they would never ask for my credit card number or Social Security number, unless I was actively purchasing something.

Recently, I think this is a spyware issue, but there was an e-mail going around asking for your satisfaction with eBay and then asked you for certain information in connection with eBay, which clearly was an identity theft kind of scam.

I think the better educated consumers are in terms of what they should expect when information is requested from them, how it works, is better. Many of the companies and associations that are going to be up later in the afternoon have had terrific activities in this area. I think that is always a critical element.

MR. FORBES: Chris, you mentioned earlier that there was some evidence that consumers were concerned about aggregate tracking as well as personal information tracking. Could you expand on that?

MR. HOOFNAGLE: Sure. There is plenty of public polling data out there articulating both concern about tracking people on an individually identifiable level, but also in the aggregate. There are technical concerns with re-identification, for instance, of anonymous data.

One of the sources for direct marketing that you see, one is actually the U.S. Census, and the minute that data is provided with identifiers stripped out, there are very smart people who can use other databases to re-identify the people, and all of a sudden, that anonymous data becomes personally identifiable.

It is important, and I said this earlier, it is important that the FTC continue to encourage people to use the anti-spyware software and firewalls.

Consumer education is likely to be of limited effectiveness more generally here. Consumer education is actually an interesting issue. It was used by the auto makers in their defense of not wanting to put seat belts in cars. They said, well, you know, most cars -- most accidents occur because of driver error. What we need is not seat belts, but driver education.

Consumer education is what we used before we had food and drug laws in the United States. It didn't work.

It makes much more sense to have the floor protections and norms set in law.

MR. FORBES: Thanks, Chris. There was a survey on consumer confusion that was mentioned earlier. Ray, could you talk a little bit about that?

MR. EVERETT-CHURCH: Sure. I've been recently involved as an expert in some litigation, and two of the plaintiffs submitted a copy of the survey which you can download from the Federal Trade Commission website for this workshop.

The survey looked into the issue of consumer confusion regarding pop up ads and the relationship between the website over which unauthorized pop up ads may appear, and without going through the litany of statistics, suffice to say that the survey showed a tremendously substantial rate of consumer confusion, both about the source of pop up ads and the attendant consumer anger and frustration with the frequency of pop up and pop under ads, and the effects upon the opinion of the brand of the website over whose web page these unauthorized ads appeared.

These have real substantial impact, not only on consumer attitudes towards those web sites whose sites are targeted by some of these ad services, but also significant impacts on the companies themselves and their

ability to control and maintain some level of consistency with regard to the consumer experience on those web sites.

Both for consumers, consumer concerns, and opinions of popular brands and for the website operators themselves, there are pretty significant negative consequences to the behavior of many of these applications.

MR. FORBES: Thanks, Ray.

Just jumping back to some of the business concerns, Jim, one of the things that companies could possibly do to assess their risk is to do a privacy impact assessment or risk assessment. Can you expand a bit upon how companies can do this to address issues related to spyware?

MR. KOENIG: I think they are more than a privacy impact assessment, but ultimately these new technologies, and assuming we are outside the definition for the workshop today, responsible businesses with legitimate purposes want to use the technology to develop long term valuable relationships with their customers and prospects.

Ultimately, that is their goal. Privacy is what they call it when they have done it wrong. When the customer, whoever they are approaching, feels encroached.

It's the balance between the business objectives and the respect for the personal privacy and making sure they respect the consumer wishes in that dialogue.

What can businesses do to make sure they have done it right? Somewhat analogous to what government agencies are required to do, they can take a look at the privacy impact of specific technology, make sure they understand the systems, make sure they understand the implications of the privacy impact and consequences and implications, as well as identify and map out the risks from a technological standpoint as well as from a business standpoint.

The next thing is once they have identified those risk areas is to make sure, and this is analogous to other parts of the law, that there is appropriate administrative, technical and physical safeguards or controls in place to make sure they manage the process. It's not just about the technology, and notice is one of the administrative things to have in place.

Until we better understand the full ramifications of these technologies and how consumers will welcome and beneficially use them over time, it's important to strike the right balance.

Companies may also want to consider for themselves to be ahead of the game, to make sure they

have different safeguards in place, potentially as mentioned before, restrictions on collection access and use of the data, but also testing and monitoring those key controls and safeguards to ensure the confidentiality, integrity and security are appropriate based on business purposes, the sensitivity of the data, and the risks identified in using this technology and the dialogue with their customers and prospects.

MR. FORBES: Thanks, Jim. A question for all of the panelists. Are there any privacy rewards related to spyware? We have been talking a lot about risks. Are there any benefits from a privacy standpoint to using technology that monitors consumers as they use the Internet or not?

MR. KOENIG: Again, back to the definition. As long as we are on the side with notice and responsible legitimate purposes, it's not necessarily the technology. It's the uses. The same technology can be beneficially used as a diagnostic tool to help analyze computer systems and to help promote inventory and inspection of computers for security protection, audit trails' accountability, but also for customer relationship management, CRM, and getting to know customers in a defined consentative relationship, to know them better.

There are benefits. It's not necessarily the

technology. It's the uses.

MR. EVERETT-CHURCH: A number of years ago, I worked for a company called Alladvantage.com, which sort of died in the dot com death spiral. The premise of the company was to collect and use consumer information for ad targeting to deliver offers and deals to folks at a time most appropriate.

The entire concept was built around explicit notice, ongoing choice of the consumer, and a very explicit enriched relationship between the company and the consumer. Consumers were not merely downloading a piece of software that they may or may not have had knowledge of what it did. They were actually encouraged through payments and rebates and getting a share of the ad revenue generated by their viewership. They were compensated for the time and real estate on their computer screens.

Now, the reality is that business failed. I think fundamentally, there remains some value there to gathering and using information about consumers' on line activities and experiences, if it can be done in a manner that is explicit and in complete control of the consumer, and works not merely to benefit them from seeing offers that they may not have seen before, but in delivering to them some substantial and real value.

MR. HENDRICKS: I had a nifty benefit from spyware. I had been writing a book on credit scores and credit reports. My teenage kid sneaks down to my computer and constantly puts Kaza on, I take it off, he puts it on, I take it off.

When I get to the point of the book where I am doing a chapter on credit repair, and I do a Google search, this shadow Google page comes up from spyware and gives me a list of credit repair outfits, and some of them claimed to have BBB on line seals, and I wouldn't have gotten that if not for the spyware.

The point is this sleazy company paid the spyware to be on the shadow page and make a claim they had this BBB seal, so I pursued that and came out with some interesting stuff in the book, which will be out next month.

(Laughter.)

MR. FORBES: Thanks, Evan. I wanted to move to a question for the panel from the audience. What is your view on notification to consumers where personal information has been compromised, do consumers have the right to know their data is at risk?

MR. HENDRICKS: Yes. That's the law in California. I've testified very strongly in favor of that. It started when the Social Security Administration

years ago had problems with the fraud rings were bribing their employees, and not just that, their information brokers, to get people's wage data.

The Social Security Administration had knowledge of Americans whose privacy was invaded, but it was their policy to refuse to notify them.

I'm very much in favor of some form of notification.

MR. FORBES: One last question.

MR. KOENIG: I just wanted to make that point that was important but all about the definition, what are the circumstances. There has been a lot of uncertainty under California and then Federal banking, interagency guidelines that address this issue, too. It's a very tricky balance that requires a lot of consideration.

MR. FORBES: Thanks, Jim. One final question, it requires a bit more broader view of privacy. How does spyware affect businesses governed by privacy laws, health care, educational professional services, et cetera?

MR. EVERETT-CHURCH: I think the Federal Trade Commission's decision in the Guess case or the settlement process there gives some information that is of use. Basically, it's expected that a reasonable organization will take measures to secure known vulnerabilities, known

risks within their infrastructure.

Clearly, this workshop should add to the amount of information out there in the marketplace that tells companies that this is a risk area, that they really ought to be addressing.

I think the FTC's guidance on that is instructive.

MR. FORBES: Thank you. I think we have time for one last question. Do you believe the recommendations made by panel one, such as labeling and uninstallation, go far enough to curb the growth of spyware?

MR. HENDRICKS: No.

MR. HOOFNAGLE: Let me mention real quickly, there are two comments, there are a lot of great comments on the record, and I spent a lot of time this weekend reading them, but there are two in particular that are worth reading that may suggest ways we can turn back this tide and get a handle over spyware.

One, of course, is the Center for Democracy and Technology's comment, which is excellent, but I would also suggest looking at Benjamin Aidelman's comments. If you read it carefully, I think in paragraph 12 he sets out what looks to me like a Section V violation for collecting personal information when they say they don't.

He has a very well reasoned piece that is worth reading.

MR. FORBES: Anyone else?

[No response.]

MR. FORBES: I'd like to thank our panelists for spending time with us this afternoon.

Please stay seated for a moment. Let's first give them a round of applause.

(Applause.)

MR. FORBES: What I would like to do is ask everybody to keep their seats. The panelists can now leave and go back to the audience.

Commissioner Thompson will be making remarks directly following this panel.

MR. PAHL: Thank you, Dean, and members of the privacy panel.

Next, we will have some remarks by FTC Commissioner Mozelle Thompson. During this six years at the Commission, Commissioner Thompson has been very active on a number of high tech issues. He's very well known in the high tech industry, and he has been involved in a variety of issues related to e-commerce innovation, including the FTC's approach to spam in the B to B marketplace.

Commissioner Thompson is the chairman of the

OECD Consumer Policy Committee, where he also heads the U.S. delegation. He is the past president of the International Marketing Supervision Network, an association of international enforcement and protection agencies.

We are fortunate that Commissioner Thompson has decided to share with us today some of his thoughts about possible responses to spyware.

Commissioner Thompson?

COMMISSIONER THOMPSON: Am I the only thing standing between you and lunch?

(Laughter.)

COMMISSIONER THOMPSON: That's not a good thing, is it?

Good afternoon. It's good to see you all. I'm Mozelle Thompson. I'm one of the commissioners here. My comments are my own today, not necessarily the views of the other commissioners. At least they were my own the last time I checked.

Welcome to our spyware workshop. You know, this one day public workshop is meant to explore issues associated with spyware. I'm happy to see so many people here from industry, government, and public interest groups to talk about these issues.

To my knowledge, this is the first broad based

public policy conference to talk about this subject, and I believe in the future, we will look back on today as a water shed event, because it will provide us with an opportunity to put a public face on what many see as secret software, and to talk about the bad and the good that can come to the use of spyware and we can identify steps perhaps that industry, government, and individuals can take to ensure that consumers have a safe, secure and enjoyable on line experience.

You all know that the FTC has long been at the leading edge of e-commerce issues. We were among the first in the world to bring consumer protection law enforcement actions in this context. To date, we have brought over 300 Internet related cases.

Along with improvements in technologies that have allowed e-commerce to grow, we have seen an increase in the sophistication of data gathering. Spyware activities can be included in that.

We also see instances where spyware can undermine consumer confidence in e-commerce. It also can impose extra costs on good actors who are forced to compete against those willing to behave unscrupulously.

Currently, reputable companies and consumers are bearing reputational risks and financial costs associated with the actions of certain spyware purveyors.

How do we address all these problems? I don't know all of the answers, but my experience at the Commission tells me that any solution must be based on transparency, on adequate notice, and consumer choice. These have been the key to on line privacy, spam, and now spyware.

Will we be able to address all of this immediately? Probably not. This is a very good start.

I would like to issue my own challenge today, because I've heard a lot of good things this morning. I would like responsible industry to come back to us with a set of best practices that will provide consumers with transparency, notice, and choice about spyware.

I would also like them to develop a plan to educate consumers and businesses about spyware, what it does, and also what it may not do.

Now, for our part here, we would like to have this be a continuing dialogue with both industry and consumers, so that government knows what kinds of actions we can take against those who would use spyware in a manner that would undermine consumer confidence. In that sense, we all have a common goal.

Welcome. We are glad to have you here. I have been learning a lot, and I expect to learn some more this afternoon, preferably after your growling stomachs can

get some attention.

Thank you very much for coming.

(Applause.)

(Whereupon, at 12:54 p.m., a luncheon recess was taken.)

1

A F T E R N O O N  S E S S I O N

MR. PAHL: Thank you very much. To start off this afternoon's events, we are going to begin with the industry responses to spyware panel. This panel will be moderated by Commissioner Mozelle Thompson.

Commissioner Thompson?

COMMISSIONER THOMPSON: Thank you. I hope you had a good lunch. The grumbling of stomachs has seemingly abated a bit. That's good.

This afternoon, I have the pleasure of participating in panel four, industry responses to spyware. We are going to try to make this a fairly interactive approach, so that we can talk to each other about what's going on out there.

Let me first introduce our distinguished panelists. Immediately to my left is Brian Arbogast, who is the Corporate Vice President of the Identity, Mobile and Partner Services Group, MSN and Personal Services Division, Microsoft Corporation. He has more than 15 years of experience in leading teams that deliver innovative software solutions and serves as an executive sponsor for privacy at Microsoft, focusing on best practices and enabling technologies as part of Microsoft's trustworthy computing initiative.

Then we have J. Trevor Hughes, who is an

attorney specializing in e-commerce privacy and technology law. He serves as the Executive Director of the Network Advertising Initiative or NAI, and the International Association of Privacy Professionals. Mr. Hughes leads the NAI's efforts to create manageable standards for industry. At NAI, he has participated in efforts to create best practices for on line profiling, the use of web beacons and cookies and e-mail marketing.

To his left is Chris Kelly, who is the Chief Privacy Officer and General Counsel of Spoke Software, a business social networking company in Palo Alto. He has more than ten years of information privacy, public policy and legal experience, including his past role as Chief Privacy Officer at the Internet Service Provider, Excite@Home.

Previously, Mr. Kelly served as an advisor in the Clinton Administration with the White House Domestic Policy Council, and the U.S. Department of Education, and was founder of the Harvard's Berkman Center for Internet and Society.

Then we have Fran Maier. Hi, Fran. She is the Executive Director and President of Truste. The Truste privacy certification seal is displayed by more than 1,200 web sites, including most of the major on line brands, and a number of Fortune 500 companies. Ms. Maier

is known for her expertise on on line privacy policies, and industry on line marketing best practices.

Then we have Andrew McLaughlin, who is the Senior Policy Counsel for Google. He is also a non-resident senior fellow at the Berkman Center at Harvard Law School, where his work has focused on law and regulation of the Internet and telecommunications networks. Mr. McLaughlin also helped to launch and manage ICANN, and currently serves as senior advisor.

Then we have Jules Polonetsky, who is AOL's Vice President for Integrity Assurance. He is responsible for a wide range of consumer protection issues for AOL's numerous brands, including advertising policy content and community standards, parental controls, children's privacy, et cetera.

Prior to being at AOL, he was Chief Privacy Officer and Special Counsel at DoubleClick, where he worked with J. Trevor Hughes and Chris Kelly for the creation of the NAI self regulatory principles for the on line preference marketing network advertisers.

Finally, we have John Schwarz, who is the President and Chief Operating Officer of Symantec Corporation, where he manages its day to day business operations to ensure the company delivers products and solutions and support that bring value to consumers.

Previously, he was President and Chief Executive Officer of Reciprocal, Inc., which provided comprehensive B to B secure e-commerce services for digital content distribution over the Internet. He also spent 25 years at IBM Corporation, where he most recently served as Manager of IBM's Industry Solutions Unit.

As I mentioned a little earlier, I think this conference provides industry with a wonderful opportunity to talk about what it does, what it doesn't do, and how it sees the spyware issue.

I had a series of questions, and I know that each of you have some things you want to show us about what you do as well. Maybe I would like to start with a question. After hearing what I heard this morning, I'm wondering what is it about spyware that keeps you up at night. What is it that gives you heartburn, that makes you anxious.

Brian?

MR. ARBOGAST: What keeps me up at night about spyware, kind of the broader category software, we categorize it as deceptive software, it is just the amount of pain it is causing customers and the fact that seems to be growing at a pretty quick pace.

To give you kind of an interesting data point, customers who send us their data when Windows crashes,

from that data, we can derive it looks like 50 percent of all crashes that are occurring to our customers come as a result of what is categorized as spyware.

If we look at where all this crash is coming from, it points to a set of files, and if you then look at the spyware tools, these files are on people's machines for the most part by a software that at least the spyware tools are saying it got there through some sort of deception, or certainly without the proper amount of notice, and amount of user choice.

We have heard a lot of the ills of spyware, deceptive software, this morning. Something we haven't talked about is the fact that all this software on the machine that the user is not aware of, there is really not much accountability for it because the customer is not aware of what is running, and it is really severely degrading the customer experience.

It is making their machine slower. It's making their machine much less stable, not to mention the things that are obvious to customers, like annoying intrusions in their browsing experience.

There is a wide range of the annoyances all the way down to things like keyloggers, that we have heard about, that are very malicious, but in general, it's kind of the breadth of the problem, and the fact that

consumers are to a large degree unaware of this.

I think you will probably hear a lot of talk about one significant component of a comprehensive approach to spyware, to deceptive software, including technological innovation, and I'm sure we will talk about that, but also consumer education.

One thing I'd like to point people to is Microsoft.com/spyware. It is where we are pointing our customers, to kind of a starting point to help us understand what is spyware, how do I know if I have it, what do I do to get rid of it, and it points to some of the tools that are out there today.

COMMISSIONER THOMPSON: What about you, Andrew? What gives you heartburn?

MR. McLAUGHLIN: Two things give me heartburn. One is that Google is victimized by a lot of these spyware applications. Actually, if we can throw up the slides, I'll show you a screen shot or two or what those actually look like.

The basic problem for us is that spyware will come along and it will hijack the Google home page or it will intercept our ad transactions.

The first one I have here is a piece of spyware called Coolwebsearch. By the way, at Google, for instance, for internal purposes, we distinguish between

spyware and what we call slimeware. We actually use a somewhat ruder name for it, but we will call it slimeware in public.

Spyware we think of as applications that export personal data off your machine. Slimeware are applications that interfere with our web services or our tool bar.

This is an example of slimeware. This is called Coolwebsearch. It appeared on October 1, 2002. It alters the appearance of the Google home page.

The way that it does this is kind of interesting. It alters the host file on a Windows computer, and it makes the Google.com translate to an address that points to the machine itself, 127.0.0.1, and it effectively acts like the web server on the machine. It coughs up results that look like this.

If you go to the next slide, you will see how this really keeps us up at night. Here are two e-mails, excerpts from two e-mails that we have.

The first one says "I've taught my 12 year old daughter to use Google and I have been shocked to find that these hijacked pages contain links to adult related sites, hosting such topics as sex toys and teen sex. I've since had to forbid her from using Google. If this continues to happen, I will simply have to strike Google

and any of its affiliates from my search tools."

This is the kind of thing that keeps a company like Google up at night.

Let's go to the next slide. This one is something called LOP or live on line portal, which is a collection of slimeware programs that attempt to drive traffic to LOP.com.

The first appearance of this was in February 2002. LOP modifies a couple of different settings. It alters your home page to go to LOP. If you try to change the home page back, LOP instead sets it to display as a new home page, whatever you choose, but with a LOP frame around it, including a LOP tool bar at the bottom.

Finally, and this is what we are trying to show here, LOP installs a tool bar, which is full of links to LOP. It hides the Google tool bar, if it's installed, and if you try to uninstall it, it keeps re-installing itself, and in fact, when you go to check the Google tool bar in your Windows' view toolbars settings, it will bring up once again the LOP tool bar.

If you go to the next slide, here are two other kinds of e-mail that keep us up at night. I won't read these. People say, man, I was faithful to Google for a number of years, but it really destroys the purpose of using Google, it's enough to put you off using Google.

Let's go to the third one. This is something called search assistant. What this does is it replaces the first page of Google results to completely irrelevant advertising links, one variant just completely replaced the ad links. Another variant actually intersperses real Google search results with their own links, so you get one real Google one, one porn link, one real Google one, one gambling link, whatever it might turn out to be.

If you go to the last slide, you will see again some e-mail that we have. It says "Hi, I've always been a loyal Google user, but for the past few weeks, whenever I search for something, I just get results from strings of advertisements. Help, please. I miss the old Google."

This is on the victim side. This is what keeps us up at night.

At the same time, Google actually makes downloadable applications. We make a toolbar. We make a desk bar. One of the other sources of anxiety is legislation that would actually make it harder or difficult for us to do the nice user friendly things that we think we can do through downloadable applications.

What keeps me up at night is the idea of poorly written legislation or unartfully drafted standards that might somehow get in the way of perfectly useful consumer

friendly services that we provide.

COMMISSIONER THOMPSON: Thank you. What about you, Chris?

MR. KELLY: Like Andrew and Brian, I worry that all client applications can get tarred with the brush of spyware. It's important to separate the good from the bad.

Spoke is an on line social networking service. We have a client download that allows you to discover relationships that you have and to strengthen a relationship profile and to talk to a central server, and who you know may know somebody that you want to correspond with and get to, and we facilitate the messages along that chain.

You can't download it by accident. You have to go to the site and download it and set it up. We have a configurable situation screen that comes up that allows you to exclude certain relationships so they never leave your machine.

The functionality that we provide, if it's labeled spyware, it is obviously quite injurious to what we are trying to do. Social networking sites, it's critical, we are always dealing with personal data to outline in fact in advance how to protect users' privacy and how we are trustworthy.

If all client downloads get tarred with the brush of spyware, that hurts our business.

COMMISSIONER THOMPSON: Jules, what are you seeing out there?

MR. POLONETSKY: I'm seeing people calling in with the kind of problem that John Gilroy, one of the Computer Guys, talked about earlier, for those who weren't here. He talked about his mom getting a copy of the new AOL 9.0 and trying to download it and not being able to, and then calling in and being told, well, okay, you are going to have to run some spyware stuff and clean up your computer so you can go ahead and download our software or other software that you want.

In addition to the millions of dollars of customer service calls, the kind of work that one needs to do, frankly, it could be an awful lot of things, people using old computers and having really bad performance for a wide range of reasons.

The cat and mouse sort of analysis that a tech will often have to do to even figure out and diagnose that this is what the user needs to do.

One of the ways that we are fighting back is by trying a little bit of self regulation of our own. If we can pull up the slide, what we will be doing in a couple of weeks and what we will be doing actually

automatically, because we don't think that most people want to become experts and want to have to take the time to track down and figure out and so forth.

I think when it comes to safety and security, users are increasingly saying do it for me, let me know what you are doing, give me some of the choices, but please do everything that needs to be done because I'm not quite sure what the definition of "spyware" is or isn't. I just want you to make it stop. Otherwise, I'm going to blame you, whoever you are.

Whoever you are often is whose phone number do I have. Do I have AOL's phone number, Microsoft's phone number. We are the people who are being blamed sometimes frankly, why is AOL sending me all these pop ups. We have made commitments, we are going to give you pop up controls, and all of a sudden, other stuff is happening, why are you lying to me.

What we are going to do is as people update to the next update to 9.0 that will be out shortly, we will automatically run what you see listed as the "scan." Then they are going to get a list. We have been very over inclusive. We are casting a wide net here, frankly.

There are items around the edge that somebody might debate, I'm good, I'm bad. The reality is what we are doing is we are going to let the users have the

transparency that the Commissioner talked about, and the notice and control over what types of applications they see, and then they can make one quick choice. They can get more detail if they actually want to know.

We also recognize there are some people who perhaps really specifically want some particular application that has made its case and it has convinced them, and while they can allow it, they may not realize that an application they have downloaded as freeware actually has something bundled they must have.

We are going to give them the opportunity to come back later when they can't run the service they want and say you know, I'm sorry, I made a mistake. I didn't realize that is what you were referring to, so I now am going to allow it. It has sort of a nice roll back. It will automatically update. It will automatically run.

When we talk about self regulation, over the years, when we were involved with the network advertising process that the Commissioner talked about, there was regulation, paying your overhead, legislation, litigation.

One of the things that actually really helped in addition to the idea that the FTC raised was the reality that there were technical solutions, P3P that was coming.

I think this is perhaps an example of where the technology is going to help press some of the best practices and self regulation, because if an application wants to remain on your computer, well, it will figure out quite well what it needs to do to tell you so that you remember it when the appropriate time comes after that scan.

COMMISSIONER THOMPSON: John, you are in an interesting position here because you have a company that gets victimized and yet you are supposed to provide solutions, too.

What are you seeing out there?

MR. SCHWARZ: We are seeing 800 million computers in use today. We are seeing half of those computers not having the most rudimentary protection against even the basic virus attacks that happen today. We are seeing technology evolve at a rate far faster than we can educate the population of people that use computers.

To go back to the first question, Commissioner Thompson, what keeps me up at night, is how do we educate people to not only buy technology and use it for good productive use, but how do we make sure they can stay productive and confident in using it.

One of the worse downfalls of these issues that

we have just talked about for the last 10 or 15 minutes is the loss of confidence in using the Internet.

Earlier today, we heard people moving away from broadband connections back to dial up connections, because they get less interrupted with unwanted or disruptive software.

We are very concerned about what's going on. We are very concerned about the user being educated adequately to keep their computers protected, and very concerned about making sure the users understand that buying a protection technology at a point in time is not adequate, that technology has to be updated constantly and continuously, and it has to be kept up to date with what is going on out there.

This, in my view, the education of that vast population of people is by far and away the greatest challenge that we face, and the greatest requirement for us as industry or you as government to jump into action and help to address this growing problem.

COMMISSIONER THOMPSON: Fran and Trevor, you both have been involved in that kind of initiative before, trying to figure out what industry can do to provide solutions, but also how do you talk to the public about what those solutions might be.

What do you think of what you have just heard?

MS. MAIER: Clearly, what we have is a big breakdown that's leading to loss of consumer trust, consumer engagement, intrusions into their privacy, potentially the transmission of personal information across a network.

It's a problem that we have to come together and address. As you mentioned, privacy has been a problem in many ways and this reminds us of the spam discussions that we have been having. There is no solution that I think stands alone. It has to have some elements of technology.

I think part of it is best practices. Best practices really serve to elevate the more responsible players, perhaps put a seal on them or some other designation, or help them work with the technology so that they don't get blocked by anti-spam filters or blocked by ISPs, put some incentives for the best practices so it makes sense for companies to raise the bar.

I think the bar needs raising. To the first question, one of the things that keeps us up is clearly, a lot of people have given consent and have had notice about things that have been downloaded to their computer, but it hasn't been effective, and it hasn't been enough.

I think we need to think about ways of making

it more specific. Maybe there are reminders, like double opt in sometimes happens with e-mail. I think there are a lot more things we can do. I think by doing those things, more companies will abide by them, hopefully, there will be some rewards for their good behavior, and hopefully there will be a way for consumers to recognize those companies who are doing it, and help them use the other technology tools to distinguish ones that aren't meeting that bar.

MR. HUGHES: Ari Schwartz mentioned this morning that it seems like every year or 18 months, we have an FTC workshop on the technology and privacy invasion of the day. It was on line privacy a few years ago. It has been cookies and web beacons and spam, and now it's spyware.

I think what we see --

COMMISSIONER THOMPSON: It's kind of nice to know we are popular.

MR. HUGHES: You are popular.

(Laughter.)

MR. HUGHES: I think what we see is a public policy process that runs its course. There are a number of tools that can be used to respond to concerns in that public policy process, technology, consumer education, best practices, and legislation.

I think depending on the issue, each one of those solutions sets offers different pluses and minuses.

What keeps me up at night right now is from a trade association perspective. Clearly, the consumer outcry over spyware is of great concern. I as a consumer and a small business person share that. My admin and receptionist just the other day, we got a notice from Roadrunner that we were about to be switched off Internet access because we were a spam drone. We had actually had to go and remove that downloaded spyware from programs on our system.

I share those consumer concerns. From a trade association perspective, I have a couple of very clear concerns. One is some of the well intentioned solutions that are in the space today create collateral damage. No one wants to buy an anti-spyware program that doesn't find anything, because then you wonder what you spent your $30 for.

As Jules said, they were over inclusive and very aggressive in stretching the definition of "spyware." I worry about that dynamic. I worry that some technologies that are otherwise benign, some companies that are trying to do the right thing, like Spoke Software or Google with their downloadable applications, or like cookies or third party cookies, get

corralled in and lumped together, and as a result, become collateral damage and the well intentions fight against something we all see as problematic.

The other concern that I have, and Chris echoed this as well, is hasty legislative responses to an emerging public policy concern such as spyware.

We have seen this now with on line privacy and with web beacons and with spam, and now with spyware. A legislative response is probably the worse first response to these tools.

On line privacy with cookies and web beacons and with spam, we have seen technology. We have seen best practices. We have seen consumer education emerge.

In some situations, legislative responses were necessary, for example, with spam. I think the legislative response really needs to be a response that emerges as the others either are succeeding with support from legislation and from enforcement, or they have failed and we need legislation to help us fix it.

COMMISSIONER THOMPSON: Do you all agree with that? I'm giving you a free one here.

MR. POLONETSKY: Yes.

(Laughter.)

MR. POLONETSKY: The over inclusiveness question that Trevor raised, I think this is sort of an

example certainly why legislation is awkward, but I think over inclusiveness has to be in the mind of the consumer.

There are some anti-spyware tools that will treat cookies as spyware. We don't, because we think telling somebody they have 850 things in spyware is not only going to scare them out of their pants, but change the nature of kind of what they think the tool is doing for them and how it is protecting them.

Others may wish indeed to know that and have a tool that does cookies plus spyware, and mentally may group it the same.

What I think all of the vendors, whether selling a vendor product or an integrated product or both, we are going to very quickly learn what consumers really think is a best practice or not by what they do when they read that list.

I think there will be a lot to learn from the debate on sort of the technical side, when people report spam or respond via the e-mail service bureaus, they are some of the best experts on what spam really is or isn't, or the ISPs. It's not necessarily tied to any particular definition.

If an awful lot of people said I didn't want it, I didn't know, I think the people who are really truly overly inclusive aren't going to be successful, and

the people who are trying to give consumers the notice and control and choice are going to find themselves a pretty good medium of what you want yanked off your computer or what you don't.

COMMISSIONER THOMPSON: Brian, what do we do now?

MR. ARBOGAST: I think the challenge that you have given us all is a reasonable one. I think we have a tremendous opportunity to pull together some of these concepts of what good behavior is and whether it's around notice, around choice.

There is one thing we can do, and that's started. A second thing we can do that we talked about is really educate customers better as to how to identify it and how to avoid it better.

Certainly one other thing we could do is get the word out and get people onto software approaches that really help protect them.

One of the things that Jeffrey, on another panel today will walk through, is some ways in which in the service part of Windows we will be basically trying to address some of the ways in which vendors really kind of try to deceive users to installing software, and basically make it a lot harder for software to be installed unless users specifically ask for it.

You see tools like pop up blocker, a tool we call the unsolicited suppressor, and what that does is just makes sure that it's not some window hiding behind the window you are looking at that is causing this to come down and get onto your machine.

There are lots of things we can do at the software level to make it harder for people, but when it comes right down to it, there are some software that you do want to be able to download off the web with clear notice.

We really do need to make sure the people understand that they need to make a call as to whether or not they want to trust the website they are currently visiting when they install software. That's the consumer education part.

COMMISSIONER THOMPSON: Earlier this afternoon, I talked about some elements, namely transparency, notice and choice. If we are talking about industry embarking on some efforts to begin to define that, for what the consumer world is like, first of all, is it doable, and which presents the biggest trouble for you?

Obviously, I think one of the reasons why we are in the situation now is because consumers really don't have a good view of what spyware is, what the benefits are, what the negatives are, and if you are

going to begin to define that world for them, partly it's going to be defining first of all your companies themselves, and collectively what that might be.

As a policy maker, I'm sitting here wondering is this doable and how long is it going to take. Part of it is getting an understanding from your part as to where you think the biggest challenges lie.

MS. MAIER: If I can answer some ideas on that. One of the issues we have been talking about all day is sort of defining "spyware" as well as defining objectionable activities. I think that is a really important first place to start.

I do think that we are going to recognize that adware is different than keylogging which is different from security and other kinds of downloadable applications.

I think it is going to be complex because we are going to have to define different notice, choice, consent, uninstall mechanisms, somewhat based upon the kind of application. There seems to be hundreds and thousands of different kinds of applications, if not now, certainly in the future.

I think it's not a simple problem. I think it does start with understanding the bad things, and I think it also has to reflect the things that we have worked

with as an industry for years called the better information practices, and really make sure we are reflecting choice, consent, transparency, redress, and using that in our tool box.

COMMISSIONER THOMPSON: John, what do you think about that approach?

MR. SCHWARZ: I tend to agree that in order to deal with the issue at hand, the most important topic is to have some definitions to help us work collectively and develop a set of best practices that we can communicate to the population at large.

As I stated earlier, the next largest challenge by far is going to be the actual education process to this 800 million human community and growing daily, on how to set their computer up in a way that makes it defensible to things we don't want to see as possible.

It is critical that we give the consumer the choice to make their own selection, their own instrumentation, their own definition of what they wish to see and what they do not wish to see, and help them understand how to then defend that installation from those things they do not wish to see.

Technology is always going to run ahead of our ability to deal with unintended consequences of the technology. As has been pointed before, rushing to

legislation is probably inappropriate at this point in time. Rushing to education, rushing to find tools that help to manage technology is absolutely appropriate, and we all have a role to play in making that happen, my company as well as the other businesses that are represented here.

I would suggest let's find a vehicle for coming together, finding common definitions, finding a way to educate the population at large through the government or through efforts the industry can undertake, and then jointly develop standards and technologies that will help to defeat these unintended consequences of technology as it races ahead.

COMMISSIONER THOMPSON: Chris and Jules and Trevor, you have been involved in this before. I may have a view about how quickly it can be done, but tell me, is this different, is spyware different?

I am also going to ask you to make another distinction. When I raised the challenge about coming up with some best practices and then the second challenge about talking to the public about them, are those two separate tasks, and do they take place simultaneously?

I'm sorry. I know that I'm talking to lawyers. You may not have figured out how to solve for multiple variables.

(Laughter.)

COMMISSIONER THOMPSON: But it's a challenge for all of us.

MR. KELLY: We'll give it a shot. I think that fair information practices and the model of the NAI principles are very good places to start in this discussion. And I think that responsible companies should come to the table the way that they have today to begin this discussion the way that they have in some prior discussions in other fora.

I think that those will continue. I think that they should continue expeditiously, and hopefully we can move to some good, solid principles that draw that line between responsible client software and spyware. Drawing that line is in the interest of every legitimate player in this industry.

So I think that that can go hand-in-hand with a consumer education campaign oriented towards explaining to people the difference between client software and spyware.

MR. HUGHES: So your first question was, you know, in self-regulatory efforts in the past that have been successful, at least in my mind, how do they compare -- are they different, were they different? And I think the answer is yes. At least when we were drafting the

NAI principles for online profiling, we knew what we were talking about. And unfortunately, I think what we've seen on the panel so far today is that largely we don't. And that work needs to happen first. We need to understand exactly what it is that we want to wrap our arms around and then go forward from there.

But that definitional work, that definition work really needs to occur first. So I think it is different. I think it's early or premature for us to be able to sit down and write best practices today without really knowing what we're talking about.

MR. POLONETSKY: I'd comment on a couple of different levels, one on the comparison to some of the other self-regulatory processes. I think one of the reasons why on the network advertising initiative side of the world things end up working is you could really could sit most of the relevant players who were doing this on any scale around the table.

They all were public or soon-to-be public companies that were, you know, part of the civil debate part of the world, and you could say to them, look, you all need to do an awful lot more to explain your business practices, because people have concerns about them. So step up, do more, work harder, bother your customers, make them do more. And since you all are interrelated

and your advertisers and your publishers are interrelated, we know that by working with the seven of you, thousands and thousands of web sites are going to have a very different privacy policy or a better notice about cookies and an opt out and so forth.

And I think that part is going to be relevant to a certain piece of the industry, you know, that you can see and find, and they'll sit in a room, and they come to FTC hearings, and you know, they want to have their business model work. And, you know, maybe the pressure one way or another way is going to help change either how they do their business or their disclosures. And I'm optimistic that there can be success there.

The other big challenge is, however, you know, like in the spam world, is that there is a huge and widespread audience that isn't going to step foot in this room or maybe, you know, anywhere near us. And there the civil, the criminal, all the other technical enforcement measures that are out there are frankly going to be necessary.

And the challenge is that you can usually, you know, figure out who's who, and the challenge in this world is you can't always yet figure out who's who. You could figure out who's who if you were there when the software was installed, but you're not always there when

the software was installed. And there are companies that were bad guys, and now they're good guys. Or they're good guys in some cases, but they're still bad guys in other cases. And we don't have as clear an audience of let's get the law abiding citizens to be better about littering and picking up and, you know, nicer about how they conduct themselves, and then people who really are, you know, running around with dangerous weapons, you know, wreaking havoc.

And unfortunately, they're sometimes wearing the same color uniforms. And so, you know, you're at risk of either technically being overinclusive in a way that frankly solves the problem but is going to need refinement.

So I think that's a little bit of a contrast with the NAI and why I think we can probably solve a chunk of the problem with best practices but are going to need a little bit more effective a tool to solve the truly nefarious part of the problem.

Just a short comment on the education piece, because I answered that in a long way. You know, the challenge again is, you know, let me go back to the computer guy's mother. There are people who want an education. All of us here who are, you know, are reasonably sophisticated whether we're very technical or

not. And we want to know. Tell me a little bit more, because, frankly, I want to know. I don't want to become a mechanic, you know, but I do want to know what the red warning lights mean. Does that mean the car is going to blow up or does that mean, okay, the oil is low, I'd better check it out at some point?

You know, kind of -- that's where a lot of us lay folks are. And so we need to educate those folks in a certain way. Here's the tool. Here's what you can buy. Here's what's free. Here's what you can do. And then there's my mother and the computer guy's mom, and they want to know which button to push to make it stop. And so the challenge is giving them that button in a way that isn't too broad, isn't too small, solves their problem in a way that's reasonable for everybody.

COMMISSIONER THOMPSON: Andrew, I know you have a response here. But I notice that one of the things Hugh and Brian are sort of in a position that if I listen to Trevor, I was wondering, how long are we going to wait to get a definition before we decide what a best practice is, et cetera, et cetera? You guys are running a business. You have to do something now, because your customers are going to go away. So are you both thinking about this differently?

MR. McLAUGHLIN: I actually think we're

probably a little bit less allergic to, you know, regulatory, legislative and other efforts in this arena. I got the --although I share a lot of the same fears and anxieties that everybody else does, but I think we're slightly less allergic.

It's really costing us money. You know, it costs us revenue. It's costing us goodwill from customers. It causes us to have to use customer support people to answer all these e-mails, give people uninstall instructions, or techies have to try to trace where this stuff is coming from. It's a real burden. We'd actually like to see something happen.

But let me say one thing, which is that I think the danger, especially in legislation, of doing something wrong rather than doing something late, is pretty serious. And let me give you just one very specific example. In a bill that was introduced by Senators Burns, Wyden and Boxer, a lot of good stuff in that bill. And I don't want anybody to take this as me trashing it. I think there's a lot of perfectly good work that went into that.

One area, though, that is less than ideal and may be harmful is that it says -- it defines as spyware anything that exports network information from your computer, and it includes the IP address, an IP address

in that definition. That means that everything that sends a packet from your computer is by definition something that is subject to the notice and consent regime in the bill.

Well, on one level, that's perfectly fine. But as a practical reality what that's going to mean is that every application on your computer is going to have you go through a notice and consent scheme for just sending packets. And that threatens to routinize the process of notice and consent so dramatically that the really bad stuff isn't being elevated to the attention of the user in the way that it ought to be.

So my point here is this. There are all kinds of I think negative things that could happen through legislation, but what this has kind of driven me back to in my couple of months at Google -- I joined in February, and I was told right when I got there, make spyware a big priority. Go to Washington and figure out what anybody's doing, and let's figure, you know, it's a real problem for us, and see what can happen.

The more that I've looked at the text of these bills that have been floating around, the more kind of nervous and worried I've become because they do seem to, you know, hold these second order consequences. And it led me to this conclusion. Even if we had a perfect law,

even if the one that I draft on my laptop tomorrow were to be enacted and signed by the President, it's not going to do us a lot of good, right. This is a tool that you can use to go after some providers.

But let's be honest. The really bad people, the ones who are responsible for the software I threw up on the slide before, are not going to be dissuaded by a law in the United States that might potentially subject them to liability here. They're not located here, right. They operate in other places, and we're dealing with a global Internet.

So this takes me back to just sort of echo something I think John said better than I could earlier, which is that ultimately, just like in the case with viruses, you don't look to the law to stop -- to really protect you from viruses. It has some tools that you can use as a company to go after people. But really, it's technology. It's my Norton anti-virus application that protects my laptop from viruses, not the law.

So, you know, I would love to see something. The sooner we can get it together, the better. The sooner we can get best practices together, the better. I'm all in favor of that. I'd like to see some urgency to that. But it does not substitute for the fact that we need to address this problem first and foremost with

better technology, better tools, user education, all the things that have been referenced on this panel.

I do want to say, though, that because we're a little bit less allergic to that stuff, I hope people will grasp the sense of urgency that we have. And I think one of the things we've got to flag is that there are bills proliferating in the states, and unless the industry is seen to be getting its act together and giving users better tools, we're going to sese bills that make people's lives harder rather than easier coming out of the states.

MR. ARBOGAST: Obviously, I feel like technology has a huge role to play, but I also am bullish on the idea of defining best practices in the industry. And I'd like to point to the work that Ari Schwartz and folks at CDT have driven in recent months.

What we found is it's easiest to identify what is clearly bad. And so I think you'll see first and foremost a consensus of what the really bad stuff is that's clearly deceptive. And to be honest, I think a lot of the laws on the books already make enforcement actions against the worst stuff possible.

And I think it's going to take a little bit more time, but it's still very doable to start to define what best practices look like. And then I think concepts

like, you know, communities rating software and consumers making use of those ratings are clear opportunities for us in this space. And so I think that technology will move ahead and will help and has to, but I also think that the industry is already kind of moving on the best practices front.

COMMISSIONER THOMPSON: Thank you. We have a few more minutes, and I have a series of questions here, some I hope the audience won't mind if I sort of condense and kind of paraphrase, because they revolve around certain kinds of subjects.

One, there are couple of questions that deal with a concern that people have about developing best practices and the concept of profit in the sense that how can we be sure that in the industry, and as the industry begins to look at best practices, that it will actually provide customers with choice and not sort of steer people to who they can get financial advantage from, or at least ensure that there is at least some competitiveness there so that one company or another doesn't wind up picking winners and losers?

MR. SCHWARZ: Let me jump in just to start. The reason I'd feel that this is not a particular danger is that it has not happened so far. There has been ample opportunity for some company to evolve to be the law-

giving single source, all fount of knowledge here, and it has not happened. Even Microsoft with their dominance in the marketplace have not succeeded in providing all of the technology necessary to be on the Internet and to use the Internet.

And so I don't think this is likely to happen in this particular domain either. What we do need to make sure, though, is that we have a set of standards that make the use of technology or use of these rules or use of the best practices as ubiquitous as possible and make those standards reasonably open so that no single company can hijack those, if you will, if that's the right word.

But I have no fear sitting here today with 25 years of experience in this world that this is likely to be a one company take all and the rest of the world is going to go scratching in the dust.

MS. MAIER: I think John makes a very good point. I think that one of the first things that any group of organizations trying to do something is to be very transparent and open about their process -- who's involved, what the rules are and so on.

I think that all of us when we think about putting together best practices want to do it in a way that we involve not only other industry players but

actually specific parts of the industry, so people from operating systems, groups from security, groups from anti-spyware technology, a wide range of industry, not just one player, and involve consumer-oriented individuals, representatives of consumers, and maybe even do some research so that we really are listening to what consumers have to say.

But I think if you get enough different kinds of groups that you have wide representation of nonprofit and consumer-oriented groups, and that you keep the process transparent, and obviously work with the FTC to get feedback, I think we'd be better off. I don't think there's a danger.

COMMISSIONER THOMPSON: I have another question here. It's a question that notes that there's been a lengthy history of consumer education on such topics as viruses and the use of anti-virus applications that what makes you think that spyware education would be more successful? And I would add a little something to that question which is, and if you think it could be, what do you think we would have to do to make it more successful?

MS. MAIER: Start with the kids. You know, just what idea is -- I brought my son here, and at risk of embarrassing him, he's the one who runs the PC. He's the one who puts the spyware on, and he's the one who's

trying to take it off.

(Laughter.)

MR. POLONETSKY: I guess I'd like to give an example from some recent experience. You know, we started talking about reducing pop-ups for our members, and we did, and people continued to complain because they were getting these pop-ups. And of course they ended up being, you know, those Windows messenger pop-ups that spammers were using to send, you know, system messages that popped up, you know, either selling anti-pop-up software, as you know, was referenced earlier, or, you know, just sort of a new kind of spam.

And so we said all right, let's tell people what this is; that it's not a pop-up, and that they can, you know, turn it off. And we'll even give them a script that they can click on. And, you know, pretty powerful message. They didn't like it. They didn't want it. You know, click here if you're still seeing a different kind of pop-up and, you know, we'll make it go away from you.

And, you know, a lot of people did and a lot of people didn't but kept calling in and costing an awful lot of money, being very unhappy about their experience and costing us an awful lot of money complaining about what was happening to their computer.

And so we said, you know what? Why don't we

just turn this thing off? Why don't we just push out a script and sort of turn it off for everybody? Tell them we've done so and they're a little healthier because of it. And if for some reason they really want this thing on because they're on a network and it's being used and forth, well then they can turn it back on.

But what I think I learned from this and others at the company as well is you've got to do that education, because there are some people who really, you know, don't mess with their settings. They want to tweak everything. And don't do anything. And then there are others where it may be appropriate to say, this truly is good for you. Nobody would argue with whether this good for your health. I'm not, you know, marketing to you. I'm turning this off. So just click the button to say, you know, don't help me today because I can cross the street myself.

So I think when we talk about this education, it's got to be, well, let's educate, but it's also, you know, get some consensus about what it's fair to say, sorry, but that's not anything that any reasonable person would want. And if they do, then, fine, let them go ahead and really specifically come back at it.

So it needs to be education with a little bit of a push perhaps.

COMMISSIONER THOMPSON: Do you agree with that, Brian?

MR. ARBOGAST: I think that clearly having smart defaults is definitely one of the things we can do to make it easier for people to protect themselves. But in the end, it is going to come down to customers making choices, and you want them to be informed choices.

So giving them the tools so that they're having the help to make an informed choice at the time that something's trying to be installed on their machine, that's the place where we can really make improvements. And that's one of the places where we've focused.

COMMISSIONER THOMPSON: Chris?

MR. KELLY: I think that process counsels towards a more expeditious and open process in the way that Fran has described to get to definitions on what are the really bad things that we're trying to target here and to separate the bad actors from the, you know, decent client software actors.

And, you know, I do applaud some of the work that CDT has done on this already and a number of other groups who are beginning to engage on it. And we need to move that process along as fast as we can.

COMMISSIONER THOMPSON: Thank you.

MR. SCHWARZ: Let me just add one other

thought. I had kind of given you a glass is half empty story up front. Let me give you a glass is half full story at the end.

Yes, we have 400-odd million users that have not taken up the anti-virus or anti-attack software. But we have 400 million users that have. And I think we can build on that base with judicious standards, with good approaches, with best practices, with constant perhaps push beyond what we have done so far. It is doable.

COMMISSIONER THOMPSON: Thank you. I notice that we're running out of time here, and I'm going to take this opportunity not only to thank you all, but also to say this. You know, those who are involved in the public policy side in the end are accountable no matter what. And you are too in the same position, because if people -- if they have a concern about spyware and they ask us, even if it's a misplaced concern or a concern that's not fully knowledgeable, they expect some action from us.

We will need something else to point people to. We will need to show what else is happening out there, how they can find resources to learn more and give consumers choices about what their experience is going to be online.

At the same time, you have many of those same

pressures, because even though you're not elected, they elect you every day when they decide whether to buy or not to buy or to participate or not to participate. And that's where we have the same challenge.

So I would say that we have an opportunity here because we're still early in the process. But the public perception is moving very quickly. So I would ask you to take that into account.

So thank you very much for coming, and we appreciate your participation.

(Applause.)

MR. PAHL: Thank you, Commissioner Thompson, and members of the Industry Response panel. We'll take a 15-minute break and begin again at quarter to 4:00.

(A brief recess was taken.)

MR. PAHL: If people could please take their seats, we'd like to begin in a minute or two. Thank you, everyone. We're about to begin our fifth panel of today, and the fifth panel will address technological responses to spyware. The moderator of this panel will be Beverly Thomas, who is an attorney in our Division of Advertising Practices here at the Federal Trade Commission.

Beverly?

MS. THOMAS: Thank you. I'd like to welcome the panel today and give them a big thank you. They

spent an awful lot of time helping educate me and prepare me for this panel. And I will introduce them, starting again to my left, Steve Bellovin, who is a member of the National Academy of Engineering an AT&T Fellow with AT&T Labs-Research. He also is co-director of the security area of the Internet Engineering Task Force.

He co-authored one of the first books on firewalls in 1994 called "Firewalls and Internet Security: Repelling the Wily Hacker", which was substantial rewritten and reissued just last year.

Jeffrey Friedberg is next. And he's Director of Windows Privacy from Microsoft. As such, he is responsible for improving the privacy experience for Windows users and identifying best practices for software development.

We then have David Moll, who is CEO of WebRoot, maker of the SpySweeper anti-spyware program.

Then is Wayne Porter, who is co-founder and primary editor for SpywareGuide.com, which distributes free and paid versions of an anti-spyware program called X-Cleaner, and also serves at the research center for specific spyware programs. He has also been active in efforts to establish a code of conduct for online affiliate marketers.

Then we have Danny Weitzner, who is a principal

research scientist at MIT's Computer Science and Artificial Intelligence Lab, and he's also a director of the World Wide Web Consortium's technology and society activities. He was the prime mover behind the development of P3P, an automated mechanism for analyzing website privacy policies.

This panel will discuss possible technological responses to spyware starting with the tools available at the desktop, then moving up to the network and ISP level, and then moving on to possible big picture changes and developments that could possibly be designed.

I think it's going to be a lively discussion because we have a bunch of techs, and techs love to talk tech, so. Before we start, though, because a lot of spyware is often stealthily installed from web pages, I've asked Jeffrey to explain how the download process is supposed to work, how spyware distributors misuse this process, and some changes that Microsoft is planning on making to reduce the inadvertent installation of spyware.

MR. FRIEDBERG: If we can have the slides up. They're there. So, as Bev suggested, it might be good just to take a quick review of how this stuff is supposed to look and then kind of go over some of the tricks and some of the new things that are coming down the path here with respect to updates to software.

(Slide.)

So here's your typical web page. This is just a simulation. It might be a news site that you like going to. And on this page there's some link down at the bottom that says, hey, here's something really cool for you to download. And it might be for something like a cool stock ticker. So you'll click on that thing, and you get the security warning.

Now the security warning comes up, and it tells you a couple of things. It says do you want to install and run, and the name of the software, in this case some ticker program. It tells you the name of the publisher, and then you have a choice of yes or no whether you want to do this.

Now you're going to get this kind of dialogue anytime you download something that could potentially run on your system. For example, just a general software program or executable, or something they call an ActiveX control. Now ActiveX control, as you may have heard them used a couple of times during the other panels, ActiveX is a plug-in to the Internet browser that extends its functionality. Its sole purpose in life is to add new capability, like, for example, better drawing. Flash is a plug-in that you might have encountered in the past.

So it's -- this kind of experience of needing

an ActiveX control or whatever or some additional software is pretty common.

(Slide.)

Now some of the common tricks that we've seen, you know, and they start from just simply confusing things to more misleading things to deceptive things, and I'll go over just a couple.

Here's a case of that same security warning, and one of the things you'll notice is that instead of a simple software name, we have suddenly a four or five line software name. I'll just read a little bit about it. It says, "After accepting our license agreements, program one, program two, two free ad-supported downloads that display (1) useful information and (2) branded ad selected based on web sites you view?"

Oh, that was a question.

"Click here to read our agreements. Click yes to accept."

Well, how many more questions will be I asked in one little space? Clearly, this was not the way this was designed. It's designed for a simple name of a piece of software, and some vendors have felt that they could put their entire end-user license agreement here. And clearly, this is confusing.

I mean, if you actually read it very carefully,

the logic is correct. And if you do click on the yes button at the bottom, it says you've agreed to all our agreements that you actually haven't looked at. Now whether this is legally binding or not is left to the lawyers. But clearly, this is confusing at a minimum, and I would dare say this is not a best practice.

(Slide.)

So there's another situation that comes up sometimes. It's called the pop under exploit. And here again, you go to that same news site, and you're looking at for a while, and then all of a sudden, that security warning pops up. And you say, you know what? Maybe this for this web page, and so I trust this web page, and therefore I might trust this download, so I might click yes; I might not.

But what you don't realize when you look at the screen, underneath there's another, you know, page that's actually in this ActiveX control, and it's that page that's actually popping this up. And this is a case of them hoping that they get lucky and that they're going to pop this security warning on top of a page that you trust, thus confusing you.

(Slide.)

This is one of my favorites. This is where cancel means yes. This has all sorts of interesting

elements in it. First off, the title. It says this is a system update. If you read a little bit further it says, no, it's a security update. And if you read even further, it says it's a privacy protection update.

Now in all cases, if you were to hit cancel or the little x in the corner, it all means yes. And the way they do this is that this is really an image. This is not a window with boxes in it. This is a picture. Now to a user and to myself, I couldn't tell the difference. But if you actually click anywhere here, you all go -- what I call all roads lead to Rome. You end up going to the site that they want you to go to to then be propositioned further and get a download.

(Slide.)

Now here's another example of the same thing. It's that window inside the window that says a security alert. Maybe you could see it. It says: Warning. Your computer is being attacked by spyware and adware. And again it presents yes, no, and cancel buttons. And of course, this is really just an image. Click anywhere on that image to make it go away, now you go back to the site and you get entrapped in their little web.

And then furthermore, down at the bottom, it says chances of you having adware software installed is 99 percent. Now I don't know how they figured that out

without really scanning my system, but clearly, you know, this is getting very deceptive here. It's quite misleading. They've provided user interface components that don't work. And I'd say, you know, time to go after these guys.

Now my mom had a similar version of this, and no one really mentioned it in the earlier panels, but it was combined with a CD tray opening up and closing. So there she was sitting there, and the CD tray is opening and closing like there's a ghost in the machine.

(Laughter.)

And up pops the window that says, if you pay us $35, we can make this go away.

(Laughter.)

Now I don't know about you, but that sounds a little bit like extortion. And, you know, clearly, it turns out that you can easily open and close the CD tray. It's a normal function of the computer. It has nothing to do with being compromised. And so here they're just trying to instill fear to get you to download the tools that they're trying to sell you.

Now my blood is beginning to boil a little bit.

(Slide.)

Now there is a couple of other ways this can get on your system. One is to accidentally leave your

front door open. This is the Internet explorer. These are the options that you actually have, and there's a slider, which is on the left there, that indicates the level of security.

Now the default that we set it to is medium, which is a very good place for it to be. Some people may want to even go higher than that. There are some scenarios where you might need to set it lower just maybe temporarily to get a particular download from a particular site that has weird permissions.

If you leave it in the low position, unfortunately, you're now exposed to drive-by downloads. This is where a web page says, hey, I've got this ActiveX control. And guess what? When you say low, that has the same meaning as saying I trust all web sites everywhere. And you won't get any dialogues, you won't get any warning. So this is a very dangerous position to leave your setting in. My recommendation is always leave it on medium or better, and if you need to set it to low, do it just temporarily and move it right back.

A couple of other things is that, you know, in general, the other ways that you might actually get software on your system is through what we've heard earlier be called security vulnerabilities. Now software systems, as we've been developing them, unfortunately

sometimes have security problems, and we've been fixing them and other companies have been fixing their problems, you know, routinely.

To avoid getting software through a security vulnerability, we strongly recommend, number one, keeping your software up to date. In this case, I would go to Windows update or turn on automatic updates. Get yourself a great anti-virus program. Make sure that's on and up to date. And these are the kinds of things. And of course, if you have a firewall, turn that on as well. And these are the things that can really help protect you from the things that are doing really malicious attacks through security vulnerabilities.

We've also heard in the earlier panels that when you get spyware on your system, they sometimes burrow and create new holes. So as you infect yourself with spyware, you're actually creating little Swiss cheeses out of your system. And, you know, do all the things that I mention, and you start to close this up a little bit, because there's companies that are devoted to trying to find those holes and fill them up.

Okay. So it turns out that in our next release of XP, which is coming out in the summer, it's called ServicePak2, there are some enhancements that can actually help address this problem. I'll go over just a

couple.

Clearly you've all had this experience. You go to a web page, oh, you get the pop-ups, and, yeah, they're for ads and whatever. It's just a common fact that pop-ups will increase your exposure to spyware. You're just being propositioned more often. There could be sites that aren't, you know, fully on the up-and-up, and who knows what they're really offering.

So we actually have included a pop-up blocker as part of the base system in IE, and it gives you both notice and choice. There's a new information bar that lies right underneath the address bar at the top where you normally see the path where you're going. And if there's a pop-up or something like that, you'll get a message that says a pop-up was blocked, and to see the pop-up, click here for additional options. And then you get some choices like, you know, look at them, et cetera, or decide to turn off pop-up blocking.

The bottom line is, you're in control. You can reduce the amount of times that you're going to be propositioned for things, and that we think is a good thing.

Next is what Brian referred to earlier as a blocker for unsolicited downloads. We know that one of the problems is that people are still barraged with, you

know, download my piece of software. Those earlier security warnings just popping up.

So we've added a blocker for those, and the logic of the blocker is that if you haven't initiated that download, if you haven't clicked on something and the page is just trying to shove this in your face, then it can get suppressed. And it goes again on this information bar that was added, and then you get a chance later to potentially act on it.

We believe this is a big advantage, because now your user experience isn't interrupted. For example, if my kids are playing with something and they get this ActiveX experience, you know, or any other executable download experience, I don't have to worry about them accidentally having to say yes to the question. They won't even get the question. It's going to be suppressed until you decide you need to go back and get one of these things.

In most cases, the page is going to tell you when it actually needs the particular ActiveX control or you're going to ask for it specifically because there's some cool functionality you want. It's the unsolicited ones that we think we need to stop.

(Slide.)

So that multi-line security warning I showed

you earlier that was confusing, which is on the left, we've redesigned the whole prompt on the right. And you'll notice that it's very clear at the very top it says, hey, do you want to install this software? Well, what software are we talking about here? Well, there's a name field and a publisher. And the name field is a fixed length. It won't go multiple lines.

So when someone tries to do something a little tricky, like trying to get their whole end-user license agreement there, it's going to turn to ellipses at the end, and it's going to be pretty obvious that someone's doing a little more than they're supposed to. The publisher is clearly identified.

And we've added a new option in this list. If you look at the one on the left, it says always trust content from the publisher. Well, in today's world, I don't think that's the best option anymore. It's unfortunate but true. We now need to have this other option that says never install software from this publisher.

So built into the system is a block list which you as a user can control. You know, if you happen to know there's publishers you don't trust, fine. Just say never install, and then you won't be bothered.

(Slide.)

And then finally, for expert users and for support professionals, there's a new add-on manager for the Internet Explorer. One of the challenges is that, well, what happens if someone did say yes at some point and you got compromised? Well, you'd like to at least go in and see what kind of ActiveX controls are installed or what kind of browser helper objects are installed. The browser helper object is the technology used to build toolbars. SO if you like downloaded the Google toolbar, it would probably show up on this list.

But you'll notice there are some on this list that look like magic numbers and stuff you don't recognize. So a support professional could go in there and help figure out what's wrong with your machine. And so this is just one of those extra steps.

In addition, once you see these things on the list, you can actually disable them. You could say, you know what? I don't know how this got here, but I'm going to turn this thing off. And people talked earlier about how hard it is to uninstall some of this software, you know, all these registry entries and all these files for 1,000, 2,000, et cetera. By going directly to where this would get called, we can actually prevent this from running. We call it neutralization.

Instead of actually removing the files, at

least it stops running and stops hurting you. And then maybe you can get an anti-spyware tool or some other tool that might go in and clean up all the mess. But at least you'd have some control right now in your own hands.

So, to wrap up, the things I just want to leave you with is, you know, definitely secure your system. The other thing is to download carefully since there is a lot of suspicious activity. Keep up-to-date anti-spyware if you can get it. And also I highly encourage people to load the new XP SP2 when it comes out since it has a number of these very nice features to help address this problem.

MS. THOMAS: Thank you, Jeffrey. I think those slides were really good in helping us understand what the problem is and some changes that might help on them.

I take it from the one that you're actually doing away with the single click download. Is that the ActiveX blocker because it's unsolicited, so you --

MR. FRIEDBERG: Well, that particular feature addresses this unsolicited situation?

MS. THOMAS: okay,

MR. FRIEDBERG: You know, whether we ever get to a place where there's enough trust where one click makes sense, you know, we'll have to see. Users still want simplicity.

MS. THOMAS: Right.

MR. FRIEDBERG: But, you know, it's hard right now because you don't know who to trust.

MS. THOMAS: And then I have another question about these downloads that a web page makes, and I want to ask our very own firewall expert here, if consumers have set up a firewall and they think, why am I getting this stuff? I have my firewall. Why isn't it stopping it?

MR. BELLOVIN: Firewalls only look at certain things, certain -- technically speaking, is they look at certain levels of the stack, and they don't look past it. Think of getting a piece of ordinary mail in your mailbox the post office is delivering. Well, you can look at the from address and to address, and that's really all the post office is looking at.

Maybe you've got a secretary who's going to go read that piece of mail and decide something, or maybe just sort this department, that department, or another level, understanding what it means. Think of how many ways you can say I love you.

Trying to understand all these different things is time consuming, expensive and extremely difficult, and most firewalls don't do it. Firewalls were aimed at particular threats. They try to block specific kinds of

things. You could build a firewall to block some of these things, but ActiveX control. Some people want ActiveX controls, and a firewall that blocked all of them would be disabled. It would be getting in your way instead of helping you.

So you can't -- it's a help. What I'd like to tell you about firewalls, it's like it says on toothpaste. It's an effective network security device as part of a program of good computer hygiene and regular professional care.

(Laughter.)

MS. THOMAS: Okay. Okay, I'd like to turn to tools that are available now at the desktop level for users to obtain. And the first are programs that scan and try and detect the spyware that a consumer has already installed on their PC.

David and Wayne, I think both of your companies offer such a product. Could you briefly explain how your product detects spyware and what it does with the spyware once it has identified it? And, David, could you go first?

MR. MOLL: SpySweeper is one of our WebRoot products, one of 13 today that's aimed at allowing an average PC user a measure of privacy and protection, and we say peace of mind as well.

The product is a signature-based product today, largely, although we see that gravitating rather rapidly. That means that it's by its nature reactionary; that we operate off of a signature file that uses spies that we trap in the wild to identify what they look like when they're on your machine, and that helps us quarantine what we find on a PC when we find it.

We really think of our product as being user empowerment. We give people a clear stated option on what to do with a piece of spyware, and that includes offering full page-long definitions of what something is, where you might have gotten it, what it can do on your system, and then of course offer you the ability to render it neutral by putting it into your quarantine and ultimately to delete it off of your system.

MS. THOMAS: Okay. Wayne?

MR. PORTER: Yes. We have two basic strategies. We have what we call the quick scan where we actually target registry keys, class IDs, window titles. We look at a number of specialized routines to get rid of some of these adwares and spywares that are very difficult.

And then we are moving -- we're beta testing now what we call DeepScan, which uses a combination of file check sums, which are mathematically secure file

properties such as size and hidden attributes as well as signature-based scanning, which lets us scale a lot faster.

When we started scanning for these back in late 1999, there was only a handful, and it was very easy to craft routines to detect them. Now, I mean, they are literally just flowing into the market like water.

The primary difference is we also -- we actually wrote a scanner in ActiveX. We designed it so -- basically, I was on a trip and I went to a public terminal and I started typing. I thought, you know, I really don't know what's here. So we designed that to be run remotely.

MS. THOMAS: So in other words, some of the -- like if you went down to Kinko's and wanted to use their computer, you could run your scanner?

MR. PORTER: Right. You can run it from wherever you were at as long as you have ActiveX enabled and you're able to use that. And there's actually been cases at Kinko's, you know, where people have installed key loggers, and that's been a big spot for identity theft.

MS. THOMAS: You both used the term "signature-based." Would one of you like to take a stab at simplifying that?

MR. MOLL: I can give it a shot. Effectively what it does, we create a digital fingerprint from a piece of known spyware, and we compare that to the files on your system.

The algorithms that we use to create those fingerprints are certain enough that if we match it, we know we've found something. So it gives us a chance to look at a PC and to know what's good and what's bad on it.

The place where things are moving, however, Bev, is really towards what we think of as sharistics. And we've seen these kinds of things happen in many ways; first with anti-virus where AV products were largely signature-based first and now today have moved towards heuristics.

We have referenced spam here I think on every panel at some point, and here's our shot now. We've moved from static blacklists for spammers to a heuristic or a means by which we can infer on a piece of spam without knowing its sender that it may in fact be an unsolicited message.

So we find that our own spyware research is moving much this way, to identify behaviors and properties that don't require necessarily a file be signaturized before we can identify it.

MS. THOMAS: Okay. You both said I think that you bring up a list or quarantine the spyware that you find. Why don't you simply remove it? Why bother the consumer?

MR. PORTER: Well, in some cases there's definitely software that the consumer wants, and we want the consumer to be empowered to make the choice. And in some cases, there's contracts that they may have entered into that, you know, we may not -- you know, we don't want to interfere with that contract they have with a third-party software.

MS. THOMAS: And this is --

MR. WEITZNER: Bev, let me just say --

MS. THOMAS: Sure.

MR. WEITZNER: That's the perfect answer. But there's a real answer under it too.

MS. THOMAS: Okay.

MR. WEITZNER: We've been talking about definition and the need or the absence of legislation today, and I think most of us think about the legislation empowering us to go out as a society to find and prosecute people who are operating outside of what we think is good behavior.

However, the absence of that legislation also leaves people who are providing the empowering tools

today, like us, at risk. And part of the need for definitional structure in this space today is to make sure that the folks who are acting on behalf of consumers and protecting everybody's mom in here apparently, have the opportunity to do that with a mandate.

MS. THOMAS: So in other words, rather than you censoring, you just identify what could be considered spyware and let the consumer decide what to do with it?

MR. WEITZNER: That's the way it is today, and I think that's right for where we are. But again, the need for definitional context here is absolutely necessary.

MR. FRIEDBERG: I'd like to add something to that. You know, as we continue to look at this problem, there's really three different types of information that is very helpful to have. One is deceptive practices, examples of them. And knowing what's bad and everybody agreeing is a wonderful thing, and that's kind of the work that CDT has started and that the FTC is very interested in.

At the other extreme, there are the best practices, which we all know is a wonderful thing for industry to adopt itself and to, you know, justify things like self-regulation, et cetera, if they call all be good actors. But what we're sort of missing is what we'll

call objective criteria. And this is really what the protection companies need in order to do their business.

They need to be able to go in, look at software objectively using some kind of criteria, assess a piece of software, and know they're not going to get a lawsuit when they put somebody on a list. And that's one of the missing pieces. And objective criteria is quite challenging. Each anti-spyware company has their own sort of definition of this, but I don't think there's an industry consensus on what that is.

MS. THOMAS: Okay. David and Wayne, just briefly, what are the limitations of scanners?

MR. MOLL: Well, I think the first and the most important relates to the fact that there's that necessary lag. You have to have one to know one at that point.

So I think that that today is a limitation to the existing scanners. Now that's going to change real quick because we've identified the kinds of things that we think make for workable heuristics, and they're rapidly approaching the marketplace. They'll be out before SP2 I think.

So we think that -- let's not confuse scanning I think with probably the desktop or the end-point security, because I think that that's really always going to be an important component of an overarching system or

a solution. So desktop needs to be, even in an ISP or a larger network view, an important component of the right solution.

MS. THOMAS: Okay. Wayne, I think you also have a product that's an ActiveX blocker, and you mentioned briefly how it works. Do you want to explain about the class ID?

MR. PORTER: Yeah. We use the class ID, which is sort of a unique identifier. And this is free. This is a spyware guide. It's free for personal use. And it can be merged right into the registry. And basically we use Microsoft's kill bit functionality, which sort of makes that program incompatible with Windows. So when they try to run it from a web page, it'll kill it. Or if it's already been installed and tries to run, it'll stop their program from running.

You know, it's not the perfect solution. There's definitely some limitations. It's more of a stopgap and it sounds like Microsoft with the ServicePak2, they're greatly going to augment that sort of functionality.

MS. THOMAS: Okay. I'd like to turn now to possible solutions at the ISP or corporate level. Because the tools we've been talking about right now, it's up to the consumer to go get them. And, you know,

some consumers are going to say, now wait a minute. I had to get an anti-virus. I had to go get an anti-spam, and now I've got to go get an anti-spyware. It's just too frustrating.

So are there possible solutions that would be more transparent to users and reduce the need for constant computer maintenance efforts by consumers? And one example, would it be possible to filter at the ISP level, maybe using ActiveX block lists or something else?

MR. WEITZNER: Can I take a crack at that, Bev?

MS. THOMAS: Sure.

MR. WEITZNER: We are today a partner of EarthLinks, and their spyware blocker takes the SpySweeper technology and moves it into their total access toolbar.

We think that that's a pretty good paradigm for a place to start today. Filtering at the network level I think is very difficult, at least for the moment. That's going to change here over time. But at least the opportunity to have an ISP step up, as AOL, and Jules is going to be out I know with something shortly as well. You can offer the functionality, keep it hosted on the desktop but make sure that for the consumer it's as painless as possible.

A tremendous amount of usability work went into

our EarthLink solution, as I know has gone into AOL's. The fact that it's paid for with your subscription makes it even easier. I think those kinds of solutions, which we've seen now work for spam, for anti-virus, pop-ups and now spyware, represent the future of what I think will be the solution here from a technological standpoint.

With the connection, you have exposure. And as John pointed out on the last pane, 400 out of 800 million to me is very much half empty, because the unprotected perpetuate the problem.

So I think the ISP standing up as they have so far represents the future here, and we for one are making sure that they have a good set of tools to do it with.

MS. THOMAS: Steve?

MR. BELLOVIN: Yes. Let me disagree at least somewhat there. ISPs are a great spot -- point of contact. The software you get from them, because they are the consumer's contact with the Internet, whatever that is. As we've heard repeatedly today, they're the people to whom many consumers turn, the other of course being their host vendor.

But you don't want to do too much in the network. For one thing, it slows it down. For another thing, you really run a real danger of stifling innovation. If you're in a situation where the only

things you can connect to from your desktop machine are things that your ISP has pronounced safe, we have to remember that the World Wide Web was not designed by ISPs. It was designed by a guy in a physics laboratory in Geneva. And it was possible on the Internet -- made the Internet that we know of today, precisely because the ISPs don't control what you see.

So there's a lot of danger. I'm not saying that there's no role for the ISPs, not by any means. I'm saying we've got to be very careful about how it's done and what responsibilities we give the ISP by regulation or statute, for fear of putting them in a position where we really don't want them to be.

MS. THOMAS: Danny?

MR. WEITZNER: Just quickly. I think that, Beverly, it's important to distinguish different types of what we might generically call ISPs. AOL offers certainly ISP service, but they clearly offer a whole lot more.

So it makes some amount of sense for them to say they're presenting you an environment that has certain characteristics that goes well beyond whether the packets flow in and out of your computer correctly. Some people want that. Other people don't. Institutions by and large don't want that, because they want to control

the way the packets flow around their institutions.

So there may be some degree of solutions from ISPs for certain kinds of environments for people who are paying their ISPs to guarantee a whole lot more about their environment, and others besides AOL do it. But as a generic matter, I agree with Steve certainly as to the web, but also as to the limitation of what the pure provider of Internet access can ever do here.

MS. THOMAS: Well, I think what David was saying was that the wy theirs works, it alerts people.

MR. WEITZNER: Right.

MS. THOMAS: To this is what you've got.

MR. WEITZNER: Yes.

MS. THOMAS: What do you want to do?

MR. WEITZNER: And that's clearly EarthLink offering a value-added service to their customers that's presumably going to make their service more attractive. So that's certainly a good thing. And hopefully --

MR. MOLL: Well, and given that the societal cost is being borne out in large part by the ISP who today takes the phone call, I think we can't blame them nor can we fight that tide that they're going to adopt solutions.

MR. FRIEDBERG: I would just like to point one other thing out. That as we learned earlier today, this

whole spywares base is quite a continuum, and there's bad stuff at one end and there's kind of grayer stuff towards the other end.

And, you know, quite frankly, I don't want someone making a decision for me whether or not a piece of badware is in my best interest or not. Maybe it's going to save me 120 bucks a year on a subscription, and that's perfectly okay with me.

So I don't know what policies are going to be put on at the ISP level. Clearly, I'd like them to stop the bad stuff. But, you know, once you get into that gray area, it gets a little tricky.

MS. THOMAS: What about corporates, corporations putting filters on their network? Different? Is that different?

MR. MOLL: I think it's equally essential, in fact perhaps more so. When we think about some of the things that we've talked a little bit about, key loggers and Trojans, you know, at the individual level we call that identity theft. But at the corporate level, that has the potential to be very serious fraud.

What happens when a payroll clerk gets that Trojan or when an accounts payable clerk gets the key logger? The potential here for harm is just simply much bigger. And in fact, I would speculate that one of the

trends we're going to see is that now they've figured out a few tricks in the spyware game, they're going to go for bigger fish. And it's not my Visa that they're going to hit. It's going to be Fidelity or Bank of America or somebody that's real scale.

So, we again are trying to architect solutions that are appropriate for those places. The consumer is still the end game here, because it's so much of our personal, financial or medical data that can be lost even in the corporate environment.

So I think that the problems here are just simply going to be bigger and more important.

MS. THOMAS: Okay. I'd like to move on to the big picture, possible tools that we might be able to develop, and I'd like to start with a P3P-like tool. And Danny, could you start by explaining briefly what P3P is and how it works in assessing website's privacy policies and then address whether something similar could be developed for spyware?

MR. WEITZNER: Sure. For those of you who don't know, P3P is the platform for privacy preferences. It's a set of technical standards deployed on the web. It's implemented in web browsers, on web servers by people who produce web sites, and it's basically designed to do one thing. It's designed to enable users of the

web to make informed choices about what kind of privacy relationships they enter into.

I'm going to spare you a lot of the technical details because time is short. But the key motivation for P3P was a recognition quite some time ago that actually came out of some of the early FTC online privacy workshops, that it's awfully hard for people, for average consumers, even not average consumers, to read privacy policies. And in fact, I would say, to the extent that that was true in 1996 or '97, it's probably all that much harder today.

We heard about the complexity of different pieces of software interacting on computers. We're well aware of the complexity of interacting privacy policies. You give your information to one place. It goes somewhere else as part of a perfectly legitimate business relationship, but you try to disentangle that through the 10-page privacy policy from the first website you visited and the 15-page policy that is on the site of the partner that you might or might not have visited, and pretty soon you get consumers who throw up their hands.

We want to try to make that simpler, to enable people who collect data to express their privacy policies in simple, machine-readable terms, and then enable users to establish what their privacy preferences are and rely

on their browsers or other pieces of software they use to help make decisions about whether the privacy relationship they're being asked to agree to is one that they're happy with or not, based on what their general preferences are.

Now I think that the key feature of P3P really was a particular kind of transparency. It was what I would call an active transparency. So it's not just having notice, but actually being able to act on the notice you get in a way that's clear and simple, and I think most importantly, doesn't take up too much of the user's time.

It's been very clear to all of us who have worked in this area that people really don't want to put a whole lot of time into these problems, into -- frankly, into managing their privacy relationships, into managing their spyware. People don't come to their computers to protect their privacy. They don't come to their computers to get rid of spyware. They come to their computers to send e-mail or write a document or do whatever they're doing.

And to the extent that you impose added costs, even with the best education programs, people simply will frankly not protect themselves very often. And when enough of that lack of protection happens, we have the

sort of network effects of problems that have been described here.

So the critical question, can this sort of approach work or help with the spyware problem? Very clearly, in the case of privacy, P3P only has helped in the privacy arena as part of a much larger view of the privacy question.

Just to take a U.S.-centric perspective for the moment, the FTC and others made it very clear that they expected, with or without law, with or without new law, that web sites would have privacy policies. They did that. Then you could start to put those privacy policies into P3P terms and people could start to make decisions based on that.

So you've got a -- we clearly have to think of this as part of a much larger question than whether there's a piece of technology, whether it's the anti-spyware technologies or whether it's some kind of labeling system like P3P, there will have to be a much larger approach. The NAI and Trustee are examples of other layers that you have to consider in the case of privacy, and I would say the same thing would have to be true in the case of spyware.

I have to say, I'm slightly on the fence here about how much a labeling approach can really accomplish

when it comes to spyware. And I think it can probably help some, but the history of trying to label things on the web I think is really instructive here. I think if you look at both privacy on the one hand and things like pornography and spam on the other hand, you see the sort of limits and benefits of labeling.

In the case of privacy, labeling clearly helped because for the most part, you had people who were collecting sites, that were collecting personal information. The legitimate ones had privacy practices that were bona fide statements of their actual privacy practices. And then people could make choices based on those statements. To the extent that spyware fits into that sort of category, that's great.

On the other hand, you have spam, where clearly spammers for the most part don't have a particularly big interest in labeling their spam as spam, and hence, all the problems that we have with spam. So you've seen with spam that the solutions tend to come in other parts of the network and frankly don't tend to rely too much on the good faith behavior of the spammers. What the solutions certainly do is they try to make it more expensive to be a spammer and make it harder to be a spammer.

So I think that's going to be an important part

of the solution here, and for better or for worse, that just doesn't have a lot to do with labeling.

As Jeffrey said, though, there is clearly a very substantial gray area of applications that might be downloaded onto a person's computer or run somewhere on the web in relation to that person's computer. And I think it's in that gray area that a labeling approach can really help a lot.

I think that clearly what's happening is that whether it's from a residential sort of consumer level ISPs like EarthLink and AOL, or through private end-user products, people are going to be putting up walls to spyware because they have to. And I actually am worried in many ways about the effect that that can have on innovation.

As it happens, some of the first P3P-enabled pieces of software, software that enabled people to read P3P policies, were plug-ins and ActiveX components, and they might well have been blocked by some of you gentlemen's spyware products with all the best intention.

So I think that it's going to be very important for the legitimate providers of downloadable applications to have some way of identifying what their applications do and enable people to make choices. Maybe people will say, don't download anything that doesn't have that kind

of label on it, so that I can make a choice. And then within that, they'll say I'm willing to download things that have certain functions but not others.

I think that operating system vendors and browser vendors can help an awful lot in working, developing best practices, developing a taxonomy of functions of applications that are downloaded and enable people to make better choices.

No one up on any of these panels today is able to make all these choices for a user. We have to give users the ability to distinguish in that gray area of things that are legal but maybe wanted, maybe not.

MS. THOMAS: I think that Steve had some thoughts on that?

MR. BELLOVIN: I'll make one comment. Labeling will work a lot better if it's something the operating system can enforce. For example, a plug-in that wants to see what URL you've just gone to, if the operating system can make sure that the only way to get to the URL is if the application has said this is what I want to do and the user has consented, and the operating system is sufficiently locked down that there's no way around it.

Figuring out the set of possible actions, the vocabulary is hard. Figuring how to lock things down is really hard, and I doubt that any operating system today

can do it. Have to depend on you guys to lock it down enough to make sure that we got the right interfaces present.

MS. THOMAS: Okay. I'd like to -- go ahead.

MR. FRIEDBERG: I just want to make one last comment. You know, I'm very encouraged by the prospect of best practices if we can more or less pursue those. And I really would like to see companies rewarded for doing and following best practices, and sometimes you may need a seal of some kind of a logo program to know very quickly whether they're following these practices.

But I know I would direct my own personal commerce toward sites and things of that nature and other applications that had the right seal on it.

MS. THOMAS: Well, I'm wondering. The security alert, the new one that you designed, that said always trust this one, could you set that only for those who are -- you know, if it's somebody who's following best practices, you could say, okay?

MR. FRIEDBERG: This is all possible once we establish the best practices and figure out what the certification programs are.

MR. WEITZNER: I'm going to just make one suggestion. I think that best practices are great if they describe a set of practices among which application

writers and users can choose.

I think that it would be unfortunate even if a diverse group, an open group, got together and said here are the things we'll allow; here are the things we won't allow. And I don't think you're suggesting that, Jeffrey, but just to be clear. Best practices doesn't mean a single list of the good things and the bad things.

Best practices I think means doing the sort of thing that the now much-mentioned CDT report -- it should have been on Amazon. It would have done really well today -- would identify a set of problematic behaviors and could identify a set of other behaviors and then let people make choices.

MS. THOMAS: Right.

MR. FRIEDBERG: Let me just clarify. On the best practices, I also see that as a continuum. And on one end there's sort of a minimum bar or a minimum level where you have to be legitimate, and that means you have to follow all the laws and not do anything illegal. You should be okay to go at that point.

Then there's the other extreme where you're doing some really extraordinary things that users really, really like. And to some extent, you should get gold stars when you do stuff like that. It's more aspirational, and may be optional, and may be more

expensive for some companies to do than others.

So you need enough latitude in the best practices so that, you know, the full spectrum of legitimate applications could get developed, and those that have the energy and resources actually can do even a better job and be rewarded in the marketplace.

MS. THOMAS: Okay. I'd like to move to another idea that I think, Steve, you brought up. Would setting up separate lockboxes for individual programs -- i.e., requiring programs to only run in their own compartment -- help reduce the problems in spyware, particularly browser hijacking or co-opting a consumer's computer for its own purposes?

MR. BELLOVIN: It is a good idea. Again, it's still in the research stage. You sometimes call them sandboxes or lockboxes. Make sure that there's a limit to what certain programs can do enforced by the operating system. It ties in again with the labeling question. You know what it can do and what it can't.

The trick is to retain the usability of the system while you're doing that. The minor part is the fact you've got to redesign all your browsers and mailers and so on. The hard part's making the system usable. Look, I'm a Unix user, so I have a very warped notion of what user-friendly is.

(Laughter.)

But, you know, I recognize there are a lot of challenges there.

MS. THOMAS: Jeffrey?

MR. FRIEDBERG: I think sandboxing that kind of strategy is actually very interesting and we should continue to look at it to see if we can get our arms around it and see if there's a way to define a ring of well-defined behavior that's quote/unquote "safe" or if something were to run in the sandbox it can't -- the mess is going to end up only being in the sandbox, not hurt anything else. That's kind of the strategy.

One of the things that we've realized -- just to finish -- is that, you know, most programs, although they can live in the sandbox, want to go a little bit beyond it. And as soon as you have one or two features that they want to do outside the sandbox, imagine needing to engage a customer saying, oh, you know, it's perfectly safe. It's doing the sandbox, but also wants to use port 25. Is that okay? I don't know how to make that trust decision as a user. And so while the technology may be there to form a sandbox, we still haven't figured out how to translate that into meaningful decisions for users.

MS. THOMAS: Okay.

MR. WEITZNER: You know, I think there's

sandboxing programs and then there's sandboxing users, Jeffrey, I think is where you're heading.

People don't want to be sandboxed. I mean, the great thing about computers is that you may say, you know, on 364 days of the year, you do want to sandbox your personal financial data from your e-mail program. It may be on the 365th day you want to send some person, maybe it's your accountant, all your financial information. And there goes your sandbox.

So I think a more -- a labeling approach that is more based on the functionality as opposed the way programmers happen to write programs would -- is probably going to be required here. Because otherwise, people will just turn it all off and say forget the sandboxes. They're too --

MR. MOLL: Well, I think there are shades of gray even here. I mean, for one, if we were all to say, great, start today, I mean, I imagine this would follow Longhorn by a few years, so we're not talking about, you know, that whole panel that couldn't sleep at night. They've got a long way to go.

I think that you can look at trusted relationships between files and applications inside the PC and start to establish the beginnings of sandboxes. They don't have to go to the ceiling to be effective

walls.

So I think there is an opportunity there that doesn't have to take place in the OS that can be sooner to market and that can be part of an overarching technological solution.

In many ways, I think there's a parallel construct here. We heard a couple of times the cry for overarching privacy legislation that takes us out of the every time we hit a border skirmish we talk about it. Today it's spyware. I suppose we can reconvene here next year to talk about fishing.

The same thing happens technologically. The long-term design of the systems and the applications that ride thereon need to be thoughtful in terms of how privacy and security get implemented. And I think things like sandboxes are really interesting, and I think that today we don't have to start at the OS to actually start to implement the concepts.

MS. THOMAS: Well, that kind of brings me to the next question about what about a lockbox for the computer's basic configuration file; i.e., the registry? For example, when a program wants to change the registry, an alert would be generated saying Program ABC wants to install itself on your hard drive, or Program ABC wants to change your browser home page. Is that okay with you?

Is that a possible idea?

MR. MOLL: From a company that just tripled its support staff in the last couple of months, I don't see that -- again, I think you can do these kinds of things from a functional standpoint. I think that the real rub comes into how you interact with the user. And that's a human user. Eight hundred million PCs speaks to who's using them. It's not just a bunch of PhDs in rooms like this. It's everyday folks. It's my three-year-old daughter.

And those kinds of warnings unfortunately create I think more often the problem of either being ignored altogether or confusing when listened to, than they solve the problem that we're trying to fix here.

MR. FRIEDBERG: I would like to just point one thing out. Unfortunately -- well, the registry is a common place for state for most programs, and there's just all sorts of stuff in there. If you were to get a message every time anything ever changed, you would never get to do your program because you'd be saying yes all the time.

And, of course, it's very hard for any individual to make those kind of trust decisions. So, clearly, the challenge would be granularity. What are the most critical elements that need this kind of

protection? We've already identified some of them. For example, your desktop user experience, especially around your Internet browsing, you know, home pages should not be hijacked. End of story. It's not something that should be allowed. And if anybody is being able to do it, then we need to find that hole and plug it immediately.

And so we have special interfaces for setting the home page which put the user in control. And if anyone's going around those, then we want to know about it and we're going to go after it.

MS. THOMAS: Well, would it be possible to just protect the most critical parts of the registry?

MR. FRIEDBERG: I think again, you know, theoretically, yes. In fact, that's part of what that exercise is -- look at those key elements, if they happen to live in the registry. Sometimes those key elements may not live in the registry. You still want to protect them.

For example, things that automatically run on the system, what's called the run key, and there's a couple of them around. Looking at those kinds of things and trying to decide what meaningful communication we have with the user about what it means when something wants to keep restarting each time you reboot your

computer, maybe that's a tipoff of what kind of program this is and what its intent is, in combination with other things.

MS. THOMAS: I want to go back to a few other possible tools available at the desktop level. What about if the user has what I'll call a rollback or a reverter, system restore type program? Will that help deal with spyware? You know, you didn't know when you got it. You now know you've got it. It's doing something to your system.

MR. FRIEDBERG: I'll actually take this one right now. My mom got that situation with the CD tray opening and closing, and she was asking what's going on. And before I had a chance really to help her, she actually used the rollback functionality on the system. I was really surprised. I don't think most people would do this. But XP has the ability to do system restore points. And every time you install something big, you could roll back to one of those points.

Now the problem of course is that you're going back in time and you're also going to get rid of other interesting things you might have loaded, like drivers for a new printer. But at least it gets you back to a stable state. So in some cases I think it could be useful. But I wouldn't call it a general tool.

MR. MOLL: Given the number of types of technological solutions we've been talking about that are either proactive or early lines of defense, this seems to me to be a station of last resort.

MS. THOMAS: Steve, did you? No?

MR. BELLOVIN: What they said.

(Laughter.)

MS. THOMAS: Okay. And one more question. Then we're going to go to a couple of questions from the audience. We heard a little bit about programs that say they're anti-spyware and they may actually be spyware, or I know that if you do a search for anti-spyware product, you're going to come up with gobs of search results. Is there a need for certification of anti-spyware programs? I.e., that they perform as they claim, such as ICSA Labs does for anti-virus software now?

MR. MOLL: I think there absolutely is. I think that this space grew up with a couple of hobbyists really behind it, and rapidly it's evolved into a pretty serious element within an overarching security space for the Internet.

The point where today we can find somebody who is capable of coding an application all by themselves, posting to a site and it's rapidly disseminating, I think places us in a position where we can tell cats from dogs,

and it's not so easy anymore. In fact, we got a piece of very inflammatory e-mail in our support group about a week ago that it completely confused us with one of the applications that is spyware masquerading as anti-spyware.

If there is not some effort -- ICSA is one point. I think COAST is another, and I think some of the guys are here from COAST today. It's the Consortium of Anti-Spyware Technologies, and I think yesterday celebrated its one-year anniversary.

So there are some beginnings. I know ICSA is thinking this over. They're not quite ready. But as soon as it can be, there could, one, be some certification of what really isn't anything other than what it's claiming to be; namely, good anti-spyware. But, two, the minute you have that definitional construct, be it for legal purposes and/or for best practices, an organization that can start to use that for a Good Housekeeping seal would also be I think a really good implementation.

MS. THOMAS: In other words, if you're going to start looking at the number of, quote, "spyware" that a program found, you need to have agreement on what's spyware?

MR. MOLL: You better believe it. I mean

that's -- the whole thing kind of hangs together.

MR. BELLOVIN: We need definitions very clearly, but I think almost more for enforcement action by the FTC and other law enforcement agencies, a certification, a company, nonprofit or whatever, only works if the consumers know to trust it. Trustee, which is the best know, is not -- my perception, and I'll be happy to be proven wrong -- is that it doesn't have great brand recognition among general consumers. I know what it is. Lots of people in this room know what it is, but I don't think most people do.

And you get spyware. The Association of Spyware Peddlers will certify things, too.

(Laughter.)

MR. BELLOVIN: Although they'll use a slightly different name. But until people know what to look for.

MR. WEITZNER: I think it's hard to find in the Internet space many examples of that really working.

MR. BELLOVIN: Yeah. That's my concern.

MR. WEITZNER: I mean, I think that people come to trust individual pieces of software either because of word of mouth or because of traditional brand-building activities. It's not really obvious to me that there are -- I think there are great sort of self-certification groups like the NAI that have come together to get

certain things done, and they certify themselves to each other. But they're really not certifying themselves to the user base that's out there.

And I think -- so I think these groups of vendors getting together has a lot of value, but it may not be the kind of value that we associate with the Good Housekeeping seal of approval.

MR. BELLOVIN: Right.

MR. MOLL: At the end, though, you know, we had Semantic and McAfee, our network associates, both up here on the dias today. I mean, that's like $20 billion worth of market capitalization right now. They've managed to establish a pretty mature industry with that Good Housekeeping seal. And I think that's, for me, the tightest analog that I can find to spyware is the anti-virus world.

MR. BELLOVIN: Well, they've got the brand names, and all the little anti-virus companies, the fact that they claim to be certified by some anti-virus organization doesn't help the consumer. They don't have the brand awareness. It's the brand awareness and the product performance over the years that has helped. And that's what it's going to take.

MS. THOMAS: Okay. Here's a quick question from the audience. This is I guess for the anti-spyware

vendors. Describe the worst case example of a security breach caused by spyware.

MR. WEITZNER: Half Life 2.

MS. THOMAS: And what did it cost?

MR. WEITZNER: Well, it caused them a launch of a hot game product before Christmas. You know, when somebody's source code gets posted to the Internet, it actually was a Q4 example where a keylogger was deposited on I believe it was the chief architect's machine, and ended up with the game source code on the web. I think that's pretty egregious.

MS. THOMAS: Okay. Wayne?

MR. PORTER: When we talk about keyloggers, I think it's important to make a distinction. You know, keyloggers can definitely be used for bad, you know, there's a large population out there who use them for monitoring their employees or they use this for monitoring their children. As a matter of fact, they're often sold as child monitors to protect them against pedophiles.

One of the most I guess worst security breaches that we saw was a very popular piece of software that was used for child monitoring, which I might add is commonly used by spouses. It's used -- we'll buy it for our child, but it's used to spy -- as a matter of fact, we've

actually seen, you know, a couple in the same household spying on each other.

(Laughter.)

It's usually the first one that wins. But in this case, the software was so poorly coded that they actually -- they used the same password. They hard coded the password. It was made for remote monitoring. So by actually buying the software, they thought they were protecting their children or spying on their wife or husband, they were actually opening up their machine, you know, wide open.

MS. THOMAS: Okay. And then the very last question. Spyware has clearly become a large problem today. Where did we as an industry fail, and what could we have done differently?

MR. MOLL: I think it's pretty early in the game to call it a failure. You know, I see the presence here is in my eyes a sign of success. We're talking about a problem that two years ago nobody in this room had heard about. We're talking about a problem with an opportunity to solve it from a policymaking and a technological and a best practices and probably a few other levels I'm not thinking about.

I'm encouraged by where we are in this thing, and I personally feel that we today have a better jump on

this than we had on spam.

So I hope that we have a more rapid success in the defense.

MR. BELLOVIN: It seems to be my role here to be disagree with people.

(Laughter.)

MR. MOLL: It usually seems to be me, Steve.

MR. BELLOVIN: I think there are a number of mistakes we can point to, but to me the biggest mistake the industry made was deploying mobile code without adequate safeguards.

The scariest thing that I heard today was it's possible to write an ActiveX control to scan a machine for spyware. You have a control that's that powerful that can roll with those permissions, my God, what else could it have done?

MR. WEITZNER: And I would just, sort of to piggyback on that. I think the mistake, if you could call it one, was to hook up hundreds of millions of PCs with operating systems that weren't really designed to work on the Internet. And there's been a huge amount of effort to catch up on that, and I think to everyone's credit who's been involved.

But it was not really expecting that there was going to be this thing called the Internet or the World

Wide Web that was going to be this extraordinarily powerful distribution medium for both content but also for malicious code.

And I don't think that's really a mistake, but I think that is the fact of the matter of where all this stuff comes from. It comes from the web. It comes from the Internet. And I think everyone's working hard to catch up to that.

MR. BELLOVIN: We'd have to go back to making an honest living, Danny boy.

(Laughter.)

MS. THOMAS: And I'm not surprised Jeffrey would like to speak, too.

MR. FRIEDBERG: I do want to point out, and I'm sure Steve can back me up on this, you know, the Internet and the Ethernet and the Arpanet, I mean, this stuff has been around for a long time. And there was originally a code of ethics with respect to use of the technology.

He's shaking his head. He knows this. And, you know, as things kind of progressed, eventually suddenly it became not just for the scientists but for the rest of the world. And as the doors opened up, so did economic incentives. And we're seeing a huge amount of that as drivers towards bad behavior.

And we've yet to have any of the right, you

know, processes in place to kind of keep that in check, and that's what this is all about I think. It's just a natural progression of what's been happening.

So actually, I really look forward to what's been going on here today, look forward to working with other industry partners on best practices and everybody else that can possibly contribute, because it's going to make my life a lot better when I use my system and my family's going to use their system. So, I think this is definitely on the right track.

MS. THOMAS: Okay. So to sum up, there are tools at the desktop that individuals can obtain to help reduce but not eliminate unwanted spyware, and it sounds like there are some technological measures that could be developed at the network, browser, and operating system levels.

However, as people have been saying throughout the day, some of these depend on establishing better definitions of spyware or some best practices.

SO it sounds like no one is there yet, but more and more companies are working on it.

So I'd like to thank you guys, and please everyone stay seated, because we're going to go straight to the next panel. So, thank you.

(Applause.)

(A brief recess was taken.)

MR. PAUL: Everyone please take their seats, please.

Thank you, everyone. We're just about ready to start our last panel of the day, which is going to be Government Responses to Spyware.

I'd like to introduce the moderator for our last panel. Our moderator is Beth Delaney. And, Beth, if you'd like to begin with the last panel, that would be great. Thank you.

MS. DELANEY: Okay. I'd like to thank everyone for staying until the very end. And also, once again, I'd like to thank our coffee sponsors for keeping us awake and alert all day, and that's the Online Privacy Alliance and the law firm of Hogan & Hartson.

For our final panel we have a very interesting group of people here, and I'm sure you're going to find them worth the wait.

We've heard a great deal of information today from a variety of different panelists, and after lunch we've been focusing on the responses to Spyware. The first panel after lunch looked at industry responses, and the second panel focused on technological responses.

This panel is going to discuss how the government can play a role in responding to concerns

about Spyware, including law enforcement, legislation, business outreach, and consumer education.

Time permitting, we'll also take questions from the audience and we'll again use the same procedure, where Shakeel is walking around, collecting the question cards. So if you have a question, write it down on a card, and he'll pick it up from you.

I'd like to start out by briefly introducing each of our panelists. On my left is Jennifer Baird. Jennifer is legislative counsel for Congresswoman May Bono of California.

In July 2003 Congressman Bono introduced the Safeguards Against Privacy Invasions Act, also known as the Spy Act.

To Jennifer's left is Mark Eckenwiler, Deputy Chief of the Department of Justice's Computer Crime and Intellectual Property Section. Mark's areas of responsibility at DOJ include federal wiretap law, computer search and seizure, and online investigations.

To Mark's left is Mary Engle, an associate director of the Bureau of Consumer Protection here at the FTC. Mary leads the Bureau's Division of Advertising Practices, which is the division that's actually running this workshop today.

The division is responsible for regulating

national advertising matters, including claims about food, over-the-counter drugs, dietary supplements, alcohol, tobacco, and online advertising.

To Mary's left is Elizabeth Prostic, who is a Managing Director with the Public Law and Policy Strategies and Information Security and Internet Enforcement Groups at the law firm of Sonnenshein, Nath & Rosenthal.

Until just last week Elizabeth was at the Department of Commerce, where she served as Senior Policy Adviser to Secretary Donald Evans and also as chief privacy officer.

To Elizabeth's left is Matt Sarrel, who's the Technical Director at PC Magazine. Matt leads the testing teams at PC Magazine, and he'll talk to us about the consumer education efforts that they've engaged in.

And last, but certainly not least, is Representative Stephen Urquhart from the Utah House of Representatives. Representative Urquhart sponsored the Spyware Control Act, which is the first Spyware legislation that was signed into effect, and that was in Utah.

And also if I could just remind the panelists, feel free to speak directly into the microphone. They're very small and you need to get up really close to them.

Let's start by finding out about current law enforcement efforts. Mary, during today's testimony we've heard about some of the concerns related to Spyware. What is the FTC planning to do to respond to these issues?

MS. ENGLE: Well, I think the first thing we're going to do is digest everything that we've heard today, and, hopefully, we won't get indigestion as a result of that. I think, actually, it's been a very good discussion and a lot of really helpful comments.

In addition, there's quite a written record, people have submitted written comments. And we'll continue and we'll look at those as well.

And then we'll have a report that we'll issue following up on this. And as people have mentioned, over the years, the Commission has held workshops on a number of these emerging technology issues, and one of the things that we hope to do is, where we see some heat going on, shed a little light on the issues. And that's one of the functions that we have here at the Commission, in addition to our role as a law enforcement agency. And we do have a couple of investigations underway right now regarding Spyware, and we would expect that those will see the light of day before too long.

We also have our consumer and business

education role to play, and as has been discussed throughout the day, there's a real need for consumer education in this area, both for parents and their kids. I mean, kids probably don't care too much about the harms that may cause, so the parents really need to know what's going on and what steps they can take.

And, finally, I think, as Commissioner Thompson had suggested, we're really interested in self-regulation in this area and best practices and working with industry to see what we can do to encourage those.

Could you just sketch out for us, what would you look for in a Spyware case, just to get everyone on the same page in terms of the different components.

MS. DELANEY: Well, to bring a case, the Federal Trade Commission would have to prove that a particular action was unfair or deceptive under the Federal Trade Commission Act. And I won't try to define those terms here, but they do have particular legal meanings, and the bottom line for both of it is that there's some consumer injury, that some harm has occurred to consumers.

And I think that that was -- I was interested to hear the discussion this morning in the first panel about defining Spyware, and there was some concern that, you know, you really couldn't come up with a definition

without inadvertently including positive software.

But for us, you know, it doesn't matter what it's called. What matters is what happens -- what happened as a result, what's the harm that's caused to consumers. And if there is harm, whether it's slowing down the consumer's PC or causing it to crash or causing them to have to reset their browser repeatedly or what have you, there are lots of different types of harm that we would find actionable under the Federal Trade Commission Act.

And so we could look at those, and then assuming we were able to identify the perpetrator -- which is an issue, and it's been alluded to earlier. A lot of times, you know, people hide themselves pretty well, and it takes a lot of investigation to actually find who is behind this, as is true in the spam arena as well, or it may be located overseas, and so that's a difficulty as well.

But I think the main thing is to -- if the practice is causing harm to consumers -- and I would say harm that's sort of quantifiable in some way, more than just sort of, well, I don't like the idea that someone may be tracking be around, and nothing really comes of it. Then we could bring a case there.

Mark, we'd like to hear about the Department of

Justice's perspective on the issues associated with Spyware. Can you first tell us a little bit about the current statutory authority that you work with?

MR. ECKENWILER: Sure. In many ways that goes back to the discussions the various panels have been having since the very beginning of the workshop this morning about the different kinds of behaviors that we're talking about when we use this umbrella term, Spyware.

From my perspective, one of the major dichotomies would be looking at subversion of a machine, taking over control, in part or in its entirety, of a particular machine, or maybe altering some setting and making it difficult to alter the setting.

That really doesn't implicate a privacy concern. You know, if I changed your home page, I really haven't impaired your personal information. I haven't disclosed something that you sought to keep confidential to someone else.

On the other hand, you may have privacy invasions. And to give you a sense of what the statutes are that would cover each of those halves, there's something called the Computer Fraud and Abuse Act, originally enacted in 1984. It's gone through a series of iterative amendments, probably about every four to six years.

One of the main prongs of that, Section 1030-A(5), speaks to impairing the integrity of -- basically it says causing damage to a protected computer, without or in excess of authorization. And as we'll discuss a little bit later, that's one of the rubs in this area.

So we certainly have a statutory tool for dealing with those kinds of subversion attacks from Spyware. In fact, that's the same statute that I would use to prosecute a denial of service attack or your typical network intrusion.

On the other side, the privacy side, there is an array of statutes that we have, depending upon the particular behavior. There's another section of Section 1030 that goes to the acquisition of data from a protected computer without or in excess of authorization. That, again, has a fairly arcane series of different elements, aggravating factors, maybe a misdemeanor, maybe a felony, depending on the circumstances.

Spyware, if it's, say, a keylogger, could in fact impact the wiretap statute, Title 3, and there's a companion statute that deals with the manufacture or trafficking, advertising of the availability of we call them interception devices. Our position would be that includes software.

And then, last of all -- this I don't think

even exhausts the list of current statutes -- there's also a statute, Section 1029, right before the Computer Fraud & Abuse Act, that deals with so-called access devices, originally intended to deal with things like stolen credit cards, but can also be made applicable to stolen passports.

So, for instance, if you have a keylogger, the keylogger may implicate not only the wiretap statute, but if there is acquisition of a bunch of passwords from the user acquired with fraudulent intent, they may also run afoul of one of the various subparts of Section 1029.

MS. DELANEY: Okay. Has the absence of specific Spyware legislation been an impediment to your law enforcement efforts?

MR. ECKENWILER: I think, by and large, the answer is no. As I think my previous answer may have communicated, we have in our quiver a number of arrows that we can use in prosecution. Let me just give you a couple actual examples.

One of the members of the previous panel mentioned the Kinkos case, a defendant named Juju Jon up in New York City who installed Spyware on a number of terminals in a Kinkos. He pled guilty last year to a five-count information, three felonies, two misdemeanors, under a variety of -- basically many of the statutes that

I just named, Computer Fraud & Abuse Act, the access device statute.

He hasn't been sentenced yet. He's going to be sentenced on May 10th. But certainly we did not experience a bar in that case.

Looking forward, just last month the U.S. Attorney's Office in Los Angeles unsealed an indictment against a gentleman named Larry Lee Ropp, accusing him of installing a keylogger on a machine at his former place of employment. And so he's now been charged with endeavoring to intercept communications in violations of the wiretape statute.

MS. DELANEY: Right. Is that the one that used the Whisteblower Act as a defense?

MR. ECKENWILER: I don't want to comment on it.

MS. DELANEY: That's fine.

MR. ECKENWILER: But, I mean, there's no defense yet. This case, you know, if it ever goes to trial, we'll find out what his defenses are. But, certainly, as I understand it, there have been some public statements about how this could -- he apparently believes it could be justified as some sort of whistleblower action. That's certainly not our view.

MS. DELANEY: Mary, I'd just like to quickly ask you the same question. Has the absence of specific

legislation been an impediment?

MS. ENGLE: No, not to this point. As I indicated, if there's harmful conduct, that's what we're going to -- or conduct that results in a harm to consumers, that's what is going to drive us, and we have adequate remedies to deal with that right now. We're not so much driven by a particular definition.

MS. DELANEY: Okay. What I'd like to do now is just to kind of move into the different legislative efforts that people are working on.

Jennifer, in a nutshell, what are the basic requirements set forth by the Safeguards Against Privacy Invasions Act?

MS. BAIRD: I'll try to put it in a nutshell. As you know, the congresswoman introduced HR 2929 in July, and we have been working on what Mary referred to and what CDT referred to earlier in the first panel regarding the difficult issues as to how to define Spyware and et cetera, et cetera.

What my boss found when she learned about Spyware is that a lot of times when people download Spyware currently, if you were to try to prosecute them or bring a law enforcement action against them, you wouldn't necessarily have any tools available just because they are giving notice.

However, it is not -- and they could easily argue that it's clear and conspicuous.

However, very few consumers actually read the notices or know what they say. So even though there is notice and there's -- you know, it's kind of check that box, that's been done, it's not effective, and people don't know what they have on their computers, and they don't know what it's doing or why their computers are running so slowly.

So what my boss's bill would do is basically require a notice regime that really puts it in the consumer's face as to what they're downloading and really asks them to decide whether or not they want to continue with the downloading process.

And that is done in a couple different ways. The first component would be a -- of course, something being included in the license agreement. The second one would be when someone is downloading Spyware onto their computer, there would actually be a downloading notice.

And what that means is, at each affirmative step that the computer user took to download Spyware, it would explain this is what this program is, it's Spyware, this is what it does, this is the information that we may collect, this is what we may do with it. If we do collect it, do you want to continue?

So it just makes it much clearer for the consumer and -- in other words, if a consumer were to consent to Spyware, technically they should never be spied on, even though it is Spyware, because they will have chosen what they want to download onto their computer and what information they want to share with another source.

MS. DELANEY: Earlier in the day it was suggested that some of the proposed legislation defining Spyware is too broad. Can you comment a little bit on that?

MS. BAIRD: Sure. This is -- as I said, this is a difficult issue as far as -- we all know that keylogging, for example, has very potential devastating effects, and that Spyware, of course, could be a magnificent tool for identity theft and et cetera, et cetera.

However, it's difficult to define Spyware to where it targets the behavior that you want to target without targeting more, without -- for example, there are -- and my boss's bill does not cover this, and neither does the Senate bill, but there are some programs that you could argue have Spyware capabilities that are great programs.

Antivirus software, for example, it has that

sort of capability to where it can see what's on your computer and what's going on so that it can prevent, you know, infection through viruses on your computer.

There are some programs that provide technical support that have some sort of Spyware capability.

And then there are the sort of things that people are saying this should not cover, and we, by no means -- my boss, by no means, wants her bill to cover that, and we have been working hard to make sure it doesn't.

I've heard a lot of different things today. I've been here since about 9:30, so -- and I appreciate that you all stayed. I was expecting the room to be empty by the time we sat up here.

But some of them were -- the first thing that the first panel mentioned, well, you have to look beyond the notice and consent, and you have to look beyond the requirement that it be easily installed, which my boss's bill does require, and you have to look at what's in the middle.

And also the argument that we need broader privacy legislation, we need a big privacy bill.

Another thing has been -- another thing that we heard from industry has been, you know, self-regulation is the answer, but we can't really come up with best

practices yet.

So, in other words, what we're hearing is, this is a problem, it needs to be solved, but we don't know how, so just hold on.

And that's not how it works in Congress, and, you know, as a member of Congress, my boss has the responsibility to do all she can to protect her constituents from downloading onto their computer that they use for personal, you know, banking and for credit -- you know, buying things through their credit card and so on and so on. She has the responsibility to make sure that they have confidence when they're using their computer, and that that information won't be shared.

And another thing that, of course, has been said is, legislation is just the wrong answer. This can only be done through self-regulation.

I would say that we can't sit around and just think about it and talk about it for days and nights in a year, we do have to act. But that being said, I do think that industry self-regulation is a very important aspect of this, and my boss understands that legislation by itself will not stop the problem, but it is a step in the right direction. It is a step in the right direction that people know what they're downloading onto their computer before they download it.

It's a very basic concept, and they should know. They should not be downloading something onto their computer that they are not aware of.

And so I guess the general message that I'm trying to get across is, something has to be done. It might not completely solve the problem, but there are some very basic things that we can do to make sure that Spyware is at least slowed down a little bit.

MS. DELANEY: I'm just going to ask you one more quick question. And if you could just tell us the major differences between your bill and the Senate's Spyblock Act.

MS. BAIRD: Okay. The Senate bill covers software in general, and when I say software in general, what I mean is the notice and consent regime does not only apply to Spyware. It applies to all software.

It also has a red herring notice which is -- implied in my boss's bill is that it's not set apart, which basically says that it is wrong to deceive or mislead someone into downloading something that they do not know that they're downloading.

Another thing is that my boss's bill only for enforcement gives the FTC the ability to enforce the bill. The Senate bill gives state attorneys general the ability enforce the law as well.

MS. DELANEY: Okay, thank you very much.

Let's move to the state perspective on Spyware legislation. Representative Urquhart, your state passed the first piece of legislation specifically directed to Spyware.

Could you first tell us a little bit about the problems that your law was designed to address?

MR. URQUHART: Sure. It was designed to address the problems that we talked about here today. First -- well, first, let me tell you some things that it doesn't do. There's a lot of myths circulating around the bill.

First is, it does not ban porn filters. Check that out on Section 1027. It does not ban instant messaging. That's clear in 102(b)(2).

So what it does so, it first addresses disclosure. If we can put up on the screen -- someone's helping me out. Here's a standard Adware disclosure. Okay, now, you look at the terms there on the bottom left, we have seven lines of text with about two or three -- you can go to the next one -- two or three words per line. Okay, thank you, that's fine.

So there that's not inviting consumers to learn about the product. That's defying them to read legalese through a straw.

You compare that to the Google tool bar here, you have many lines of text appearing on a screen. Now, this first one, this is to protect Google and their property. So you can go to the bottom there and just hit, okay, I agree with that.

Go to the next one, please.

Now, this is one protecting consumers. Look up at the top there in the red. They're pointing out this is not the usual yada yada. They're begging people to read their disclosure policy. Then down there at the bottom you have to click on a feature. So you're forced to actually pay attention and do some reading.

Now, there's a world of difference between those two.

So in this area what we did, and what we would encourage policymakers to do would be to study consumer knowledge and perceptions, and we've heard today that 75 percent of the people with Adware don't know they have it, they don't know how they got it. So we can't call those people consumers; they're victims.

So I would say a law legitimizing current practices would be a significant step backward. So we, first off, beefed up disclosure. Secondly, we addressed removal. We've had a lot of discussion on that today, so I won't discuss that.

I'll go to my third and last point, which is -- we deal with context-triggered popovers, and these are ads triggered based on the content of a web site without any affiliation to that web site.

And so the policy question here is, is this good old-fashioned American competition or is it parasitic? And we concluded unanimously that it is parasitic, and the host of that parasite is commerce.

And we concluded that Adware threatens commerce in two ways. First, it hobbles the Internet. When users are burdened, frustrated, even frightened by undisclosed invaders, then they're going to avoid that technology. They're going to shy away from e-commerce.

And, secondly, we think that Adware destroys -- and I'm talking Adware under current practices, like the first disclosures you saw. It destroys investment-backed expectations. So, again, policymakers here had to weigh the burdens and benefits to commerce.

Now, I'd encourage you to think of a lemonade stand. Commerce values the legitimate competition of several more lemonade stands. That's good. Commerce does not value the illegitimate competition of stealing lemons out of the orchard. In the marketplace of e-commerce, the lemon grove is planted and tended by web site owners and affiliated marketers, and currently

they're being harmed.

You've got to remember that in the short term, the best deal for consumers is shoplifting. Nothing beats the five-finger discount. But in the long term, if investment-backed expectations are trampled, then the marketplace and consumers will suffer.

And vendors need a little space in the marketplace. That's why the butcher, the baker, the candlestick maker, they have little expectation for privacy out in the public, but in their shop, no one can camp out at the cash register. And if they're allowed to do this, then the market will shift solely toward the harvest. In other words, the market will shift solely toward stealing purchases at the point of purchase, and it will move away from planting and tending the orchard, and that would be developing and branding a web presence.

So those are the things that we addressed. I really enjoyed hearing Jennifer's comments. I agree with them 100 percent. I think that unless there is regulation in this area, the butcher, the baker, the candlestick maker, they'll stick to brick-and-mortar if their sales can be stolen at the point of purchase in one context, and not the other, and then consumers also will shy away from this wonderful technology.

MS. DELANEY: Could Utah's state tort law,

something like interference with a prospective business or customer relationship, have been able to deal with some of these issues rather than additional legislation?

MR. URQUHART: Arguably they might have. Or especially if you have a statute like California's Unfair Business Practices Act, that might be able to.

But I think that that is a horrible way to make law, because those are very blunt instruments. I mean, it's just something unfair that you don't like, and it wasn't created with the Internet in mind. And as a result, it would be left up entirely to the courts to flesh out policy and flesh out law in this arena, and a better way to do it is to have legislatures specifically look at all the things and use a nuanced approach, which is what we did, and at the end of the day, it bans bad behavior and leaves the good actors alone.

I mean, we've heard a lot today about Adware, how it really bogs down people's computers. It's really a problem. Well, we've had one Adware company say that my bill, even though it hasn't gone into effect yet, has cost them tens of thousands of downloads. There are a lot of happy consumers out there by that fact.

Another Adware company that is about to go public, they have in their S-1 statement that because of this law, they're going to avoid Utah. That's great.

I mean, constituents, they demand results. They're sick of this stuff. And so I've heard a lot of handwringing here today, and I think it is great that we do need best practices, we need education, we need technology, but we also need regulation.

I mean, how do you stop bad guys? You have a neighborhood watch? You have education to pick up your newspapers. Don't leave them sitting around. You have technology, you have alarms and bars, but at the end of the day, you've got to have laws and a cop on the beat. And so we've put a cop on the beat.

MS. DELANEY: So just to recap, the major requirements for your bill -- or your law is notice and consent, a removal aspect, and then the context-triggered pop-ups?

MR. URQUHART: Right. So the bulk of industry, they're fine, because if they do monitor data, if they mine data, then they can provide some consent on that and easy removability.

Now, if they do context-based advertising, then there are some significant additional requirements for notice. Tell them what kind of pop-ups they're going to get, how often they're going to get them, and we don't allow them to pop over at the point of purchase.

MS. DELANEY: Are there any points you've like

to make in comparing your legislation to the different federal legislative efforts?

MR. URQUHART: Well, I'm excited about Representative Bono's bill. I think that that's a wonderful start. We need to empower consumers. They need to know what they're getting into.

I mean, right now we have an arms race. You've heard that Whenu has been removed 80 million times. The business model there, it's just to dump it on computers faster than people can become educated and get it off.

And so that's a very important component.

But I think we fall short if we don't deal with the context-based advertising. I think this is very detrimental to e-commerce. E-commerce, just like we do in the real world, you have to defend and back up investment-backed expectations.

And so that's an aspect that I would hope the federal -- you know, at some point the federal government's going to preempt this, and I don't pretend that that's not going to happen. But I hope they do it with a beefy, good bill that protects consumers and commerce.

MS. DELANEY: Before we move on to outreach to the business community, do any of the other panelists have any comments on what we've covered so far? Okay.

Elizabeth, can you tell us about the Department of Commerce's efforts to work with the business community in responding to the concerns and issues raised by Spyware?

MS. PROSTIC: Sure. Let me first say that I promised Secretary Evans that I would be on my best behavior since I left the Department four days ago.

One of the things that the Department has done under Secretary Evans' leadership, as with past secretaries, is be the advocate for the private sector, promote economic growth -- particularly here we're talking about e-commerce -- and, third, support international trade.

And I think that Spyware plays a role in all of those. As we learned in the spam context, you can't just regulate it here, you have to talk about what happens abroad.

But what we've done predominantly is open our doors to the private sector and the privacy advocates and to really focus on the larger policy questions, which are balancing the need to protect the privacy of individuals and businesses, while preserving innovation and some of the legitimate practices that the private sector is endeavoring.

And this is similar to the approach we've taken

on other types of -- in other technologies. With spam, as many of you were here for that evolution, we looked at specific solutions to privacy, self-regulatory approaches, technology solutions, and then, in the end, congress decided, with administration support, that there was legislation needed to track down some of the bad actors, giving the FTC and the Department of Justice authority to enforce certain penalties.

So, really, what we've done is to try to open our doors, try to listen to the private sector and to the privacy advocates, and to ensure that we are taking into account some of the larger principles that are specific to Spyware that are not unlike other technology issues that we faced in the past.

MS. DELANEY: Have there been specific harms that have been visited upon businesses? Have you heard much from the business community in that regard?

MS. PROSTIC: Well, absent legislation, I think that many legitimate businesses are focusing on what current practices could be curtailed, or could be prevented if legislation is enacted, but it doesn't take into account certain definitions or certain practices. So I think it would be hard to pinpoint a specific practice.

But, really, right now we're focusing on trying

to differentiate between practices and activities that are good for consumers and those that harm consumers, and that there's a need to legislatively punish certain violators, in addition to the existing statutes that the FTC and the Justice Department have at their discretion.

MS. DELANEY: What I'd like to do now is turn to Matt Sarrel. Matt, as I mentioned before, is the technical director at PC Magazine.

First, can you tell us a little bit about why PC Magazine focused that much attention on this issue?

MR. SARREL: Well, we -- we took our first in-depth look at Spyware in April of 2003 in an article entitled "Spyware, it's Lurking on Your Machine." So, that was a year before this article that you're mentioning now. And that article focused on describing the risks and prevalence of Spyware -- really defining the problem. Defining what Spyware is, key loggers, Adware, ad cookies -- things like that. And then we went on to review several anti Spyware solutions.

Prior to that, we had been looking at the overall issue of Spyware, particularly key loggers, as a lot of them are considered to be viruses for many years. And overall, our readers look to us for guidance in understanding how to deal with the serious nature of the Spyware problem. Our readers really want to understand

the effects of Spyware. They want to detect and remove Spyware from their systems.

So, at the beginning of this year, we spoke with a lot of analysts who were reporting an explosive growth in both the types of Spyware, and the number of computers infected with Spyware. So we decided the issue was worthy of a large cover story.

So then, in March -- well actually, I guess, in January, because it takes us a long time to actually get into print -- we started working on the story that you had there, called Spy Stoppers. It was within a larger package that also contained information regarding identify theft and safe computing. This time, we changed our focus a little, and we felt that we had described the problem fairly thoroughly, and what we did instead was focus on reviewing 14 anti-Spyware tools, and we included several side bars about how to recognize the symptoms of Spyware, and also how to avoid becoming infected in the first place.

We feel that the magnitude of Spyware and the issue of Spyware increases as more and more people integrate Internet usage into their daily lives, and that consumers or victims have a right to understand the issue, and what they can do to protect themselves.

MS. DELANEY: Right. We've heard a lot about

consumer education today, and what I'd like to ask you next is -- you know, from your unique perspective, what can you tell us about what government agencies and consumer advocacy groups need to keep in mind when designing effective consumer education initiatives?

MR. SARREL: Okay. Well, first, I want to say that I think everyone here -- what I've heard today has been good in terms of, you know, best practices on the part of the industry, legislative controls, but in my mind -- and it -- you know, of course, it's because of the way that I approach the problem as being involved in consumer education. So, what I think first has to happen is that consumers need to get sick and tired of having this garbage put on their machines. And when consumers can't stand it anymore, that's when something's going to get done, because they're not going to buy the things, they're not going to download the things that come with Spyware.

So, along with that comes with -- that I think, in the beginning, what we need to do is educate consumers about what is at stake, and why people should care. So, after we did these two stories, I got so many e-mails from people saying that they didn't care. Who cares? Fine, so there's Spyware on my machine. But, you know, I'm able to download music for free. You know, that I'm

willing to make that trade. And I just -- that -- that kind of shocked me, and I even had a discussion with one person who said that she didn't care if a certain item of software was Spyware -- she finds it to be a convenient took for completing web forms.

So, I asked her if she would buy a stolen Rolex on a street in Manhattan, hand the guy a business card, ask him to put her name and address in a data base, and then periodically send him updates on her jewelry purchasing habits. So, I think she got it after that. Consumers need real-world examples of these risks to their personal information. A lot of them feel that there's anonymity in numbers, and that they're safe, because it's over the Internet.

So, you know, why doesn't everyone just e-mail me their credit card and PIN. People seem to understand that. Right, there's been credit card fraud, people have adjusted their level of understanding to understand, or include, credit card fraud. I think part of their problem is, they just don't get Spyware, and, you know, what it -- what it can do to them.

Someone earlier drew the analogy between Spyware and computer viruses, and I think that that's appropriate. And I think back to when I was a network administrator in the early 1990s, and I saw my first

outbreak of some boot sector virus that's, you know, probably long gone. I tried to educate my users how not to get viruses, how not to bring them into the work place, things like that, and no one got it. Okay? But now, 15 years later -- well, we'd like to think everyone's running anti-virus software, and that people get it. And hopefully, it won't take 15 years to understand what's wrong with Spyware.

So, I think also, in computing, consumer education usually starts with the media. People read an article about something, they become interested about it. Also, people tend to learn things when they go to buy something. And also, people learn from their corporate IT departments. So, you know, PC Magazine and PCMag.com provide a lot of educational material, as do anti-Spyware and anti-virus vendor web sites, and various government sites. There are also specialized web sites that focus on security and privacy issues, including the latest Spyware information, education, and detection and removal tools.

Corporate IT departments should train employees -- just like they did with anti-virus software -- they should train employees, and distribute tools to detect and eradicate Spyware, especially on mobile systems, in addition to teaching people how to use software

firewalls. And finally, retailers should have virus, Spyware, Malware information centers, or kiosks, subsidized by software vendors.

And then the final note I'd like to leave everyone with is that my -- my gut feeling that all the education in the world won't do anything until consumers understand the real risks to personal information inherent to Spyware.

MS. DELANEY: You know, that's a great point, because I think we had a phone conversation a couple of weeks ago, and as horrible as some of these virus outbreaks have been, you thought that actually, some of them were kind of helpful in the sense that they -- they made consumers more aware of what was going on, and that actually forced them to buy some of these products, and -- or download them for free, just to deal with the problem.

MR. SARREL: Right. That's what -- you know, I get a lot of -- it's funny, I gain a lot of understanding from talking to my friends, or my parents' friends, about the problems they have with their computers, right? So, what do they have? They have pop-ups. They have -- the machine's running slowly, they don't understand why. You know, maybe they have -- they have got a worm that's using up all their band width. But they don't understand

that. What -- what they understand is, they -- they can't do what they want to do.

And for now, my comment about the viruses, because a lot of these worms don't really carry a lethal payload. So, they're -- they're sort of just people trying to get attention. And, you know, when they get attention, they disrupt the way that you use your machine. And what I'm -- what particular concerns us is that somewhere in between all of these things spreading so easily and so quickly, is going to come something that has a big payload. Or, the Spyware that, you know, really takes everything away from you. And I think people need to understand what the risks are, and just get -- be sick of the risks, and take the precautions that they need before anything really happens.

MS. DELANEY: We have some questions from the audience, so I'll give -- Does any other panelist want to add anything at this point, before I move into that? We have -- the first question is for Mark. "You mentioned a few cases where use of a key logger was prosecuted. Have there been cases where authors have been investigated or charged, and is there a legal framework to use for authors under current law?" So it would be the -- the people that were writing the key loggers.

MR. ECKENWILER: You could, in theory, bring a

prosecution under Section 2512. Certainly, it's a more attractive case from a prosecutive standpoint, if you have the person actually trafficking in it, and actually making this available as a commercial product for sale, actually deployed out in the market place. So yes, I think, you know, in -- in most cases, we would have a -- a mechanism for going after someone at least who's trafficking. I'm -- I'm not sure that 2512 would apply strictly to someone who just created such a product.

And of course, the -- the thing to remember is, there are other -- there are interception tools all over the place, many of which are used by system administrators, just to do network diagnostics, so there -- there is certainly a -- I'd say it's a fine line, but in fact, it's a very fuzzy line, there, about what's -- what's appropriate and what's inappropriate in terms of monitoring software.

MS. DELANEY: We have a question for Jennifer. "Since Justice and the FTC both said that no new law is needed to prosecute where consumer harm can be shown, what is the need for your bill, specifically?"

MS. ENGLE: Can I interrupt, and just say, I was not speaking for the FTC --

MS. DELANEY: It's too late.

(Laughter.)

MS. ENGLE: -- or any individual commissioner, or the FTC staff.

MS. BAIRD: Well, I think that the answer to that question is kind of a sub-section under the general Spyware problem, and that gets back to what I was saying earlier. You -- it's hard to prove that there's been any harm or wrong, if, for example, someone's computer has just slowed down, or if they, you know, have to wipe off everything that's on their computer and start all over. You know, that's -- there's not any monetary damage there, and there isn't any -- any personally-identifiable information per se that has been taken because of it.

However, the Congresswoman would argue that that is, in fact, damage, and that that should be included under Section 5-A of the FTC Act, as an unfair deceptive act, since the consumer, when he or she downloaded it, had no idea that by downloading it, they would cause such things to happen to their computer. And if course, you know, no notice is going to say "If you download this, it might slow down your computer," however, it will say "This is what the purpose of this software is. This is it's function, this is what it will collect, and this is what we will do with it."

And so, the idea is -- and you know, it's surprising to hear what Matthew says, but I believe it.

I believe that there are some people who actually would continue with the downloading process. That's why my boss doesn't necessarily say that Spyware should be prohibited, but instead, consumers should have the choice to decide whether or not they want to download it. And when they make that decision, they should have -- they should be informed as to what they are deciding.

And, of course, as I mentioned before, this -- this requires a combination of legislative action, as well as self regulation and industry, and just, you know, consumer education in general by all entities interested and involved in Spyware.

MS. DELANEY: "Representative Urquhart, your bill exempts operating systems from the definition of Spyware. As you are probably aware, there has been a lot of litigation about what is bundled, or integrated into a dominant operating system. Is it your understanding that an application that is bundled, integrated into the dominant operating system is not covered -- for example, Windows Media Player, while others, for example, Real Player or Apple Quick Time, would be covered?"

MR. URQUHART: Yeah, let me point out that, in Utah, like in most states, we don't write our laws into -- in stone. We don't chisel them in stone, we write them on paper, and so, we have made it plenty clear to

industry, and to all parties, that we wanted their input. And about the only input we got during the sessions was, don't do it. Let -- for Heaven's sake, let the feds deal with this, and, you know, that -- that's not acceptable to my consumers. And so, this was brought forward by an industry member, saying put in an operating system, and currently, in the law, they could argue that this is a vital component of the operating system, then it would be exempted out.

But, you know, if someone were wanting to make the case, then they could go through all the detailed criteria, stating otherwise, that it does monitor activity, that it sends information about the -- the computer use, it doesn't provide adequate disclosures, and it's not easily removable. So, you know, to answer your question, I -- I think currently, the way the law is written, those would not be covered by the law.

MS. DELANEY: Okay. I have another question, here. I think you did touch on this, but I'll -- I'll ask it, and you can have an abbreviated answer if it's been fully covered. "How are, for example, Utah contact lens consumers harmed by receiving a point of purchase pop-up from another vendor with lower prices on the same item?"

MR. URQUHART: Well, again, if you could

guarantee that it were lower prices, that would be a different issue, but there's no guarantee there what's going is -- in the case of contact lenses, again, you have someone with stuff on their computer, and they're just bombarded by advertisements. No one says that it is a better deal. It's just stuff that they didn't consent to have it there, and so, it just keeps popping up, and they should have a say. So again, it goes back to consent.

They're -- they're harmed by the fact that it is using up the resources of their machine, and then the contact lens company would also be harmed, if it came on, and someone was just triggering off their site, they've spent all the money to invest in that site. Maybe an affiliated marketer has pushed someone to that site, they also have invested, and so then, if, at the point of purchase, someone pops right in, well, there's very little investment that went into that. And that's why the profits of these Adware companies -- the profit margin is just unbelievable. I mean, the only comparable thing with a similar profit margin is crime. You know, one crow bar, and -- and you're in business.

And so, here that -- that again is my point, that if we allow this conduct to happen, then all efforts are pushed just to the harvest, and not to actually

building the business.

MS. DELANEY: And then, I think we have time for one more question. This one is for Mark. Although, Representative Urquhart, you, by far, have the most questions. But I'll spare you. Mark, "If a user is unaware that a software application is running on their PC, can it still be argued that they have agreed to the license agreement?"

MR. ECKENWILER: As a lawyer, I can tell you that anything can be argued. And, in fact, that's -- that's one of the -- one of the challenges in this area, I think. I -- I don't -- I don't want to be on record, I actually agree with Mary that I -- I don't think my position -- since I don't speak for the Department of Justice, the U.S. government, or Major League Baseball here today, is that no legislation in this area is at all appropriate.

I think the point is well taken that, if we were to try to charge somebody with, you know, a Computer Fraud and Abuse Act violation for putting up -- you know, one of these "Do you want to accept this" screens that's, you know, 25 pages long in six-point type, in a very narrow column, totally unreadable, it's not the most attractive circumstance for us to bring a criminal prosecution, remembering that we actually have a

Constitutional burden to prove beyond a reasonable doubt that, as I said before, this was under 1030, without or in excess of authorization.

I think the first line of defense in such a case is going to be that the defendant was, in fact, acting within the scope of authorization, and that becomes a kind of ugly jury question. If we're going to pick and choose cases to prosecute, I think we are more likely to take cases like the Jon case, or this newly-indicted case, the Ropp case, where there just -- there's no argument that that was -- there was never any constructive notice. Never even any attempt at notice. This was, you know, purely a -- a clandestine installation.

So, yeah, it could be argued, it -- it's -- it is certainly a consideration, deciding whether or not to -- to bring a case.

MR. SARREL: Hey, I wonder if you could just ask the jury if they've ever read a license agreement.

MS. ENGLE: And can I just follow up on that from -- from our perspective. The FTC law is pretty clear that, if you're going to give notice to consumers of something, it has to be clear and conspicuous, and we have actually issued a long -- you know, several years ago now, guidance to the online community called "Dot Com

Disclosure," that gives you a pretty good understanding of how to make disclosures clear and conspicuous to consumers, and that includes things like, if they've got to click on a button to find out the information, that the button has to be clearly labeled, and also, labeled with the import, so that they know why they should be clicking, not -- not just click here for more info, or something like that. So, from our perspective, just because some term is buried in a four-page ULA doesn't mean that consumers have necessarily given their consent to it.

MS. DELANEY: Great. Does anybody else have anything to add before we finish up? I'd like to ask everyone in the audience just to stay seated for a moment. We're going to have closing remarks from Director Beales. I think -- the panelists, can we sit down, or should we stand here? I think panelists can go back to their seats, but if everyone in the audience could remain seated.

(Applause.)

MR. PAHL: Well, thanks, Beth, and -- and to the members of our Government Response panel. The last, but certainly not least part of our program today is some closing remarks by BCP director, Howard Beales. Howard?

MR. BEALES: Thanks, Tom, and -- and thanks to

all of you for sticking around. We've reached the end of an important, and, I think, productive workshop. I want to thank all of the panelists who volunteered their time and expertise to discuss the varied and complex issues related to Spyware.

I'd like to thank those of you who were not panelists, but who provided public comments, or posed questions to direct our discussions, and helped us to build a rich and detailed record. The record remains open for public comments until May 21st. Please use this opportunity to submit a comment in response to what you've heard today. The instructions for submitting a comment are on the FTC Spyware Workshop web page, that's FTC.gov/bcp/workshop/spyware.

I particularly wanted to thank Commissioner Swindle and Commission Thompson for participating in the workshop. Their leadership has been, and will continue to be, critical, as the commission assesses what is Spyware, what problems it might cause, and the merits of possible solutions to these problems. And last, but certainly not least, I'd really like to thank the staff of the Division of Advertising Practices for their exemplary work in organizing this workshop.

The panels this morning were a spirited and informative discussion that will give us a better

understanding of what Spyware is, and the problems that Spyware may cause. This afternoon, we heard a vigorous debate about the many options available to the government, to industry, and to consumers, to respond to Spyware. Today's discussions will provide important grist for the mill as we consider possible responses to the issues that Spyware raises.

Let me offer some thoughts based on what I've heard today. It seems clear from today's discussions that there is software that may cause privacy, security, and functionality problems for consumers. The FTC's privacy agenda focuses on the misuse of consumer information, and the explicit recognition of trade-offs in our information economy. But consumers may not understand the trade-offs related to Spyware.

Spyware may harvest personally-identifiable information through monitoring computer use, without their consent. It may also facilitate identity theft by surreptitiously planting a keystroke logger on a user's personal computer. It may create security risks, if it exposes communication channels to hackers. It may also affect the operation of personal computers, causing crashes, browser hijackings, home page resettings, and the like. These harms are problems in themselves, and could lead to a loss of consumer confidence in the

Internet as a means of communication and confidence. And in commerce.

Second, many of the panelists discussed how Spyware may cause problems for business, too. Companies may incur costs as they seek to block Spyware from the computers of their employees. Employees will be less productive if Spyware causes their computers to crash, or they're distracted from their tasks by a barrage of pop-up ads. Spyware that captures the keystrokes of employees could be used to obtain trade secrets, and other confidential information from businesses.

Because of the novelty of Spyware, there's been little empirical data as to the prevalence and magnitude of these problems, for consumers or businesses. But some of the potential risks are severe, and government, industry and consumers should take steps to keep these problems from spreading. Fortunately, we hear this afternoon that substantial efforts are currently underway to address Spyware. In response to market forces, industry is developing and deploying new technologies to assist consumers.

Consumers and businesses are becoming more aware of the risks of Spyware, and they're responding by installing anti-Spyware products, and other measures. Today, certain industry representatives indicated that

they would explore best practices and consumer education on issues related to Spyware. Government and industry-sponsored education programs, and industry self regulation, could be instrumental in making users aware -- or more aware -- of the risks of Spyware, thereby assisting them in taking actions to protect themselves.

These approaches let consumers choose the trade-offs that work for them. I think that all of these efforts are very encouraging. Although there are several efforts underway to address the issues and concerns created by Spyware, we must take -- we must carefully and clearly define the problem. Spyware is an elastic and vague term that has -- that it has been, and could be, used to describe a wide range of software.

A vague definition of Spyware could be so broad that it covers software that's beneficial, or benign, software that is harmful, software that is beneficial or benign but misused, and software that is just poorly written, or inefficient code. Such imprecise definitions would treat these types of software in the same manner. We need to determine whether there is a definable class of software that can truly be called Spyware.

The easiest way to start drawing lines is case-by-case law enforcement. We have had investigations in this area, and we will have more. But we need your help.

When you see bad practices, please tell us. And please tell us whatever you know about who is engaged in these bad practices. We're taking names.

This workshop has generated a tremendous amount of information for the commission, and for the public to evaluate, relating to Spyware. I'm confident that the workshop will assist government, business, and consumers in developing effective and properly-focused responses to Spyware. Thank you again for coming, and for devoting your time and effort to making this workshop happen. Thank you.

(Applause.)

(Whereupon, at 5:51 p.m., the workshop was concluded.)

* * * * *

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

DOCKET/FILE NUMBER: _____

CASE TITLE: FTC v. _____

HEARING DATE: _____

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: May 14, 2004

_____

PETER SHONERD

# 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