

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

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

1		
2		
3	Opening Remarks - J. Howard Beales, Director, Bureau	of
4	Consumer Protection, FTC	10
5		
6	PANEL ONE: DEFINING, UNDERSTANDING, AND	
7	DISSEMINATING SPYWARE	
8	Moderator: Thomas B. Pahl, Assistant	
9	Director, FTC	13
10	Panelists:	
11	Ari Schwartz, Associate Director, Center	
12	for Democracy and Technology	16
13	Ed Black, President and CEO, Computer	
14	and Communications Industry	
15	Association	17
16	Mark Bohannon, General Counsel and	
17	Senior Vice President for Public	
18	Policy, Software and Information	
19	Industry Association	18
20	Marty Lafferty, Chief Executive Officer,	
21	Distributed Computing Industry	
22	Association	19
23	Avi Naider, President and CEO, WhenU.com,	
24	Inc.	20
25		

1	Remarks Concerning Risks of Spyware -	
2	Orson Swindle, Commissioner, FTC	62
3		
4	PANEL TWO: SECURITY RISKS AND PC FUNCTIONALITY	
1	Moderator: David K. Koehler	67
2	Panelists:	
3	Maureen Cushman, Legal Counsel, U.S.	
4	Consumers, Dell	69
5	Bryson Gordon, Senior Manager, Product	
6	Management Group, McAfee Security,	
7	Consumer Division	71
8	Roger Thompson, Vice President, Product	
9	Development, Pest Patrol	75
10	Michael Wood, Vice President of Sales, USA	
11	and Canada, Lavasoft	75
12	John Gilroy, Technology Contributor for The	
13	Washington Post and Co-Host, WAMU's	
14	"The Computer Guys" program	77
15	Austin Hill, Co-Founder and Chief Privacy	
16	Expert, Zero-Knowledge Systems	94
17		
18	PANEL THREE: PRIVACY RISKS	
19	Moderator: Dean C. Forbes	112
20		
21		

1	Panelists:	
2	Chris Jay Hoofnagle, Associate Director,	
3	Electronic Privacy Information Center	116
4	Evan Hendricks, Editor-Publisher, "Privacy	
5	Times"	117
6	Ray Everett-Church, Chief Privacy Officer,	
7	Turn Tide, Inc.	119
8	Ronald Plessner, Piper Rudnick, LLP	123
9	James H. Koenig, Chief Practice Co-Leader,	
10	Privacy Strategy and Compliance,	
11	PricewaterhouseCoopers, LLP	125
12		
13	Remarks Concerning Possible Responses to Spyware -	
14	Commissioner Mozelle Thompson	152
15		
16	PANEL FOUR: INDUSTRY RESPONSES TO SPYWARE -	
17	INDUSTRY BEST PRACTICES AND WORKING WITH THE	
18	GOVERNMENT	
19	Moderator: Commissioner Mozelle Thompson	156
20	Panelists:	
21	Brain Arbogast, Corporate Vice President,	
22	Identity, Mobile and Partner Services	
23	Group, MSN and Personal Services	
24	Division, Microsoft Corp.	159
25		

1	Andrew McLaughlin, Senior Policy Counsel,	
2	Google	161
3	Chris Kelly, Chief Privacy Officer and	
4	General Counsel, Spoke Software	165
5	Jules Polonetsky, Vice President, Integrity	
6	Assurance, AmericaOnline, Inc.	166
7	John Schwarz, President and CEO, Symantec	
8	Corp.	169
9	Fran Maier, Executive Director and	
10	President, TRUSTe	171
11	J. Trevor Hughes, Executive Director,	
12	Network Advertising Initiative	172
13		
14	PANEL FIVE: TECHNOLOGICAL RESPONSES TO SPYWARE	
15	Moderator: Beverly J. Thomas	197
16	Panelists:	
17	Jeffrey Friedberg, Director of Windows	
18	Privacy, Microsoft	199
19	Steven Bellovin, AT&T Fellow with AT&T	
20	Labs-Research	212
21	David Moll, President, WebRoot	213
22	Wayne Porter, Co-Founder and Primary	
23	Editor, SpywareGuide.com	214
24		
25		

1	Daniel Weitzner, Technology & Society	
2	Doman Leader, World Wide Web	
3	Consortium; Research at MIT	217
4		
5	PANEL SIX: GOVERNMENT RESPONSES TO SPYWARE -	
6	LAW ENFORCEMENT, CONSUMER EDUCATION, AND	
7	COORDINATING WITH INDUSTRY	
8	Moderator: Beth Delaney	251
9	Panelists:	
10	Mary Engle, Associate Director, Division of	
11	Advertising Practices, FTC	254
12	Mark Eckenwiler, Deputy Chief, Computer Crime	
13	and Intellectual Property Section,	
14	Department of Justice	257
15	Jennifer Baird, Legislative Counsel, Office	
16	of Rep. Mary Bono	261
17	Stephen Urquhart, State Representative,	
18	Utah House of Representataives	267
19	Elizabeth Prostic, Chief Privacy Officer, U.S.	
20	Department of Commerce	274
21	Matthew Sarrel, Technical Director, PC	
22	Magazine	276
23		
24	Closing Remarks - J. Howard Beales, Director,	
25	Bureau of Consumer Protection, FTC	291

P R O C E E D I N G S

- - - - -

1
2
3 MR. PAHL: Good morning, and welcome to the
4 FTC's Spyware Workshop. My name is Thomas Pahl. I'm an
5 Assistant Director in the FTC's Division of Advertising
6 Practices here at the FTC.

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

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

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

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

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

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

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

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

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

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

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

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

25 Prior to becoming Bureau Director in 2001,

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

8 (Applause.)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

24 (Applause.)

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

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

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

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

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

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

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

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

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

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

20 Welcome to our panelists today.

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

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

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

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

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

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

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

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

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

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

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

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

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

25 Our association has not yet signed on to this,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 experience over the Internet.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

11 What's happened recently is that as other forms
12 of software-based advertising have proliferated,
13 particularly ones that have been perceived as threatening
14 to certain types of businesses on the Internet and that
15 have sparked some litigation and other things related to
16 the protection of business interest, the definition of
17 Spyware has actually become very, very complicated.
18 Because it's now used to address not just programs that
19 monitor or secretly record behavior, as was in the mid-
20 '90s, but it's now used to try to be all-inclusive and
21 threaten what are some very legitimate technologies in
22 other types of software-based advertising.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 should be considered to be a type of Spyware.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14 MR. PAHL: Certainly.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 P2P file-sharing applications?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

25 Obviously, we and many folks on the Internet,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

25 (Applause.)

1 (A brief recess was taken.)

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

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

17 (Videotape is played.)

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

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

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

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

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

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

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

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

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

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

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

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

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

1 practices and notices, without legislation.

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

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

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

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

23 Thank you very much.

24 MR. PAHL: Thank you, Commissioner Swindle.

25 Now what I'd like to do is introduce the

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

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

8 Thank you.

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

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

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

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

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

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

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

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

13 Last but not least is Michael Wood, who is Vice
14 President of Sales for USA and Canada, Lavasoft, who has
15 been distributing anti-spyware products since the late
16 1990s, including a free program called Ad-Aware.

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

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

1 spyware, and whether you see a trend here.

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

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

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

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

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

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

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

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

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

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

25 Unfortunately, this complaint can easily and

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

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

8 MR. KOEHLER: Thank you, Maureen.

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

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

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

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

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

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

19 If you look at the last eight months, the
20 number of adware applications that McAfee has actually
21 detected on an user's system is just under 40 million,
22 with the spike coming actually just now in March with
23 11.4 million being detected on the user system.

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

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

7 This chart we have right now, this is actually
8 the growth in spyware, adware, keyloggers, and various
9 other potentially unwanted programs since August of last
10 year, and it is showing that growth in things other than
11 the sort of core adware has been relatively flat.
12 However, when you look at the sheer numbers of detection,
13 these have been normalized for consumer growth, for
14 subscriber growth, but if you look at the sheer numbers,
15 things like web dialers, the fact that we have detected
16 4.2 million web dialers in the past eight months, and
17 when we have customers calling in telling us I have a
18 \$5,000 phone bill and I don't know what to do about it,
19 it's showing these types of sort of non-viral threats are
20 becoming a very serious problem for consumers.

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

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

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

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

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

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

24 MR. KOEHLER: Thank you.

25 Asking Roger and Michael, have these trends

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

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

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

11 MR. KOEHLER: We will get to that.

12 MR. THOMPSON: Absolutely, it's accelerating.

13 MR. KOEHLER: How about Lavasoft?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

25 I think it's a serious problem and it costs

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

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

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

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

19 It is a huge problem.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

22 MR. KOEHLER: What would that be?

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

1 coming in.

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

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

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

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

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

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

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

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

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

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

24 MR. THOMPSON: That absolutely happens.

25 MR. KOEHLER: Roger, you mentioned something

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

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

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

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

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

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

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

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

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

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

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

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

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

1 ability to evade --

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

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

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

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

25 MR. THOMPSON: That's not doing anything

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

3 MR. WOOD: Exactly.

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

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

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

24 Any transmission of the information really
25 constitutes a security hole.

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

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

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

21 MR. WOOD: I definitely concur with that.

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

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

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

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

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

17 MR. HILL: Sorry.

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

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

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

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

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

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

1 computer isn't acting like it should.

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

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

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

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

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

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

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

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

23 Michael, would you like to start off?

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

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

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

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

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

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

1 bounds.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5 QUESTION: Can we ask questions?

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

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

14 (Laughter.)

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

22 (Laughter.)

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

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

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

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

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

1 bill is so high.

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

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

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

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

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

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

6 MR. WOOD: Exactly. I concur with that.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8 Thank you very much.

9 (Applause.)

10 (A brief recess was taken.)

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

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

22 MR. FORBES: Thank you, Tom.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

25 My first question is going to be to Chris, Evan

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

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

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

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

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

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

1 think that there actually needs to be increased
2 regulations to deal with the invasiveness of advertising.
3 65 percent reported that they thought advertising was out
4 of control.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

21 (Laughter.)

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

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

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

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

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

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

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

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

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

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

25 On the privacy issues, the way you defined it,

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

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

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

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

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

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

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

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

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

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

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

25 It is a problem that hits all of the businesses

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

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

7 MR. FORBES: Thanks, Ron. Evan?

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

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

23 MR. FORBES: Thanks. Thanks, everyone.

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

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

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

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

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

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

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

1 themselves.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 give you notice and will obtain your consent.

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

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

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

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

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

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

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

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

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

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

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

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

1 to make their own informed decisions.

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

11 It's a place to start.

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

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

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

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

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

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

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

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

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

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

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

23 MR. FORBES: Thank you, Ron.

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

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

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

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

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

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

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

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

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

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

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

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

16 (No response.)

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

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

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

25 MR. KOENIG: We touched on some of the things

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9 MR. FORBES: Thanks, Ray.

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

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

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

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

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

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

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

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

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

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

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

25 There are benefits. It's not necessarily the

1 technology. It's the uses.

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

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

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

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

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

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

17 (Laughter.)

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

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

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

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

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

9 MR. FORBES: One last question.

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

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

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

1 risks within their infrastructure.

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

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

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

13 MR. HENDRICKS: No.

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

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

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

3 MR. FORBES: Anyone else?

4 [No response.]

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

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

9 (Applause.)

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

13 Commissioner Thompson will be making remarks
14 directly following this panel.

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

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

25 Commissioner Thompson is the chairman of the

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

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

9 Commissioner Thompson?

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

12 (Laughter.)

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

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

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

25 To my knowledge, this is the first broad based

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

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

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

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

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

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

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

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

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

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

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

1 get some attention.

2 Thank you very much for coming.

3 (Applause.)

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

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

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

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

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

6 Commissioner Thompson?

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

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

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

25 Then we have J. Trevor Hughes, who is an

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

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

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

21 Then we have Fran Maier. Hi, Fran. She is the
22 Executive Director and President of Truste. The Truste
23 privacy certification seal is displayed by more than
24 1,200 web sites, including most of the major on line
25 brands, and a number of Fortune 500 companies. Ms. Maier

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

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

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

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

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

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

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

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

18 Brian?

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

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

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

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

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

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

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

1 consumers are to a large degree unaware of this.

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

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

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

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

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

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

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

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

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

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

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

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

1 and any of its affiliates from my search tools."

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

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

8 The first appearance of this was in February
9 2002. LOP modifies a couple of different settings. It
10 alters your home page to go to LOP. If you try to change
11 the home page back, LOP instead sets it to display as a
12 new home page, whatever you choose, but with a LOP frame
13 around it, including a LOP tool bar at the bottom.

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

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

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

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

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

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

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

1 friendly services that we provide.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

12 What are you seeing out there?

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

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

25 One of the worse downfalls of these issues that

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

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

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

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

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

25 What do you think of what you have just heard?

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

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

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

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

25 I think we need to think about ways of making

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

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

16 I think what we see --

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

19 MR. HUGHES: You are popular.

20 (Laughter.)

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

1 I think depending on the issue, each one of
2 those solutions sets offers different pluses and minuses.

3 What keeps me up at night right now is from a
4 trade association perspective. Clearly, the consumer
5 outcry over spyware is of great concern. I as a consumer
6 and a small business person share that. My admin and
7 receptionist just the other day, we got a notice from
8 Roadrunner that we were about to be switched off Internet
9 access because we were a spam drone. We had actually had
10 to go and remove that downloaded spyware from programs on
11 our system.

12 I share those consumer concerns. From a trade
13 association perspective, I have a couple of very clear
14 concerns. One is some of the well intentioned solutions
15 that are in the space today create collateral damage. No
16 one wants to buy an anti-spyware program that doesn't
17 find anything, because then you wonder what you spent
18 your \$30 for.

19 As Jules said, they were over inclusive and
20 very aggressive in stretching the definition of
21 "spyware." I worry about that dynamic. I worry that
22 some technologies that are otherwise benign, some
23 companies that are trying to do the right thing, like
24 Spoke Software or Google with their downloadable
25 applications, or like cookies or third party cookies, get

1 corralled in and lumped together, and as a result, become
2 collateral damage and the well intentions fight against
3 something we all see as problematic.

4 The other concern that I have, and Chris echoed
5 this as well, is hasty legislative responses to an
6 emerging public policy concern such as spyware.

7 We have seen this now with on line privacy and
8 with web beacons and with spam, and now with spyware. A
9 legislative response is probably the worse first response
10 to these tools.

11 On line privacy with cookies and web beacons
12 and with spam, we have seen technology. We have seen
13 best practices. We have seen consumer education emerge.

14 In some situations, legislative responses were
15 necessary, for example, with spam. I think the
16 legislative response really needs to be a response that
17 emerges as the others either are succeeding with support
18 from legislation and from enforcement, or they have
19 failed and we need legislation to help us fix it.

20 COMMISSIONER THOMPSON: Do you all agree with
21 that? I'm giving you a free one here.

22 MR. POLONETSKY: Yes.

23 (Laughter.)

24 MR. POLONETSKY: The over inclusiveness
25 question that Trevor raised, I think this is sort of an

1 example certainly why legislation is awkward, but I think
2 over inclusiveness has to be in the mind of the consumer.

3 There are some anti-spyware tools that will
4 treat cookies as spyware. We don't, because we think
5 telling somebody they have 850 things in spyware is not
6 only going to scare them out of their pants, but change
7 the nature of kind of what they think the tool is doing
8 for them and how it is protecting them.

9 Others may wish indeed to know that and have a
10 tool that does cookies plus spyware, and mentally may
11 group it the same.

12 What I think all of the vendors, whether
13 selling a vendor product or an integrated product or
14 both, we are going to very quickly learn what consumers
15 really think is a best practice or not by what they do
16 when they read that list.

17 I think there will be a lot to learn from the
18 debate on sort of the technical side, when people report
19 spam or respond via the e-mail service bureaus, they are
20 some of the best experts on what spam really is or isn't,
21 or the ISPs. It's not necessarily tied to any particular
22 definition.

23 If an awful lot of people said I didn't want
24 it, I didn't know, I think the people who are really
25 truly overly inclusive aren't going to be successful, and

1 the people who are trying to give consumers the notice
2 and control and choice are going to find themselves a
3 pretty good medium of what you want yanked off your
4 computer or what you don't.

5 COMMISSIONER THOMPSON: Brian, what do we do
6 now?

7 MR. ARBOGAST: I think the challenge that you
8 have given us all is a reasonable one. I think we have a
9 tremendous opportunity to pull together some of these
10 concepts of what good behavior is and whether it's around
11 notice, around choice.

12 There is one thing we can do, and that's
13 started. A second thing we can do that we talked about
14 is really educate customers better as to how to identify
15 it and how to avoid it better.

16 Certainly one other thing we could do is get
17 the word out and get people onto software approaches that
18 really help protect them.

19 One of the things that Jeffrey, on another
20 panel today will walk through, is some ways in which in
21 the service part of Windows we will be basically trying
22 to address some of the ways in which vendors really kind
23 of try to deceive users to installing software, and
24 basically make it a lot harder for software to be
25 installed unless users specifically ask for it.

1 You see tools like pop up blocker, a tool we
2 call the unsolicited suppressor, and what that does is
3 just makes sure that it's not some window hiding behind
4 the window you are looking at that is causing this to
5 come down and get onto your machine.

6 There are lots of things we can do at the
7 software level to make it harder for people, but when it
8 comes right down to it, there are some software that you
9 do want to be able to download off the web with clear
10 notice.

11 We really do need to make sure the people
12 understand that they need to make a call as to whether or
13 not they want to trust the website they are currently
14 visiting when they install software. That's the consumer
15 education part.

16 COMMISSIONER THOMPSON: Earlier this afternoon,
17 I talked about some elements, namely transparency, notice
18 and choice. If we are talking about industry embarking
19 on some efforts to begin to define that, for what the
20 consumer world is like, first of all, is it doable, and
21 which presents the biggest trouble for you?

22 Obviously, I think one of the reasons why we
23 are in the situation now is because consumers really
24 don't have a good view of what spyware is, what the
25 benefits are, what the negatives are, and if you are

1 going to begin to define that world for them, partly it's
2 going to be defining first of all your companies
3 themselves, and collectively what that might be.

4 As a policy maker, I'm sitting here wondering
5 is this doable and how long is it going to take. Part of
6 it is getting an understanding from your part as to where
7 you think the biggest challenges lie.

8 MS. MAIER: If I can answer some ideas on that.
9 One of the issues we have been talking about all day is
10 sort of defining "spyware" as well as defining
11 objectionable activities. I think that is a really
12 important first place to start.

13 I do think that we are going to recognize that
14 adware is different than keylogging which is different
15 from security and other kinds of downloadable
16 applications.

17 I think it is going to be complex because we
18 are going to have to define different notice, choice,
19 consent, uninstall mechanisms, somewhat based upon the
20 kind of application. There seems to be hundreds and
21 thousands of different kinds of applications, if not now,
22 certainly in the future.

23 I think it's not a simple problem. I think it
24 does start with understanding the bad things, and I think
25 it also has to reflect the things that we have worked

1 with as an industry for years called the better
2 information practices, and really make sure we are
3 reflecting choice, consent, transparency, redress, and
4 using that in our tool box.

5 COMMISSIONER THOMPSON: John, what do you think
6 about that approach?

7 MR. SCHWARZ: I tend to agree that in order to
8 deal with the issue at hand, the most important topic is
9 to have some definitions to help us work collectively and
10 develop a set of best practices that we can communicate
11 to the population at large.

12 As I stated earlier, the next largest challenge
13 by far is going to be the actual education process to
14 this 800 million human community and growing daily, on
15 how to set their computer up in a way that makes it
16 defensible to things we don't want to see as possible.

17 It is critical that we give the consumer the
18 choice to make their own selection, their own
19 instrumentation, their own definition of what they wish
20 to see and what they do not wish to see, and help them
21 understand how to then defend that installation from
22 those things they do not wish to see.

23 Technology is always going to run ahead of our
24 ability to deal with unintended consequences of the
25 technology. As has been pointed before, rushing to

1 legislation is probably inappropriate at this point in
2 time. Rushing to education, rushing to find tools that
3 help to manage technology is absolutely appropriate, and
4 we all have a role to play in making that happen, my
5 company as well as the other businesses that are
6 represented here.

7 I would suggest let's find a vehicle for coming
8 together, finding common definitions, finding a way to
9 educate the population at large through the government or
10 through efforts the industry can undertake, and then
11 jointly develop standards and technologies that will help
12 to defeat these unintended consequences of technology as
13 it races ahead.

14 COMMISSIONER THOMPSON: Chris and Jules and
15 Trevor, you have been involved in this before. I may
16 have a view about how quickly it can be done, but tell
17 me, is this different, is spyware different?

18 I am also going to ask you to make another
19 distinction. When I raised the challenge about coming up
20 with some best practices and then the second challenge
21 about talking to the public about them, are those two
22 separate tasks, and do they take place simultaneously?

23 I'm sorry. I know that I'm talking to lawyers.
24 You may not have figured out how to solve for multiple
25 variables.

1 (Laughter.)

2 COMMISSIONER THOMPSON: But it's a challenge
3 for all of us.

4 MR. KELLY: We'll give it a shot. I think that
5 fair information practices and the model of the NAI
6 principles are very good places to start in this
7 discussion. And I think that responsible companies
8 should come to the table the way that they have today to
9 begin this discussion the way that they have in some
10 prior discussions in other fora.

11 I think that those will continue. I think that
12 they should continue expeditiously, and hopefully we can
13 move to some good, solid principles that draw that line
14 between responsible client software and spyware. Drawing
15 that line is in the interest of every legitimate player
16 in this industry.

17 So I think that that can go hand-in-hand with a
18 consumer education campaign oriented towards explaining
19 to people the difference between client software and
20 spyware.

21 MR. HUGHES: So your first question was, you
22 know, in self-regulatory efforts in the past that have
23 been successful, at least in my mind, how do they compare
24 -- are they different, were they different? And I think
25 the answer is yes. At least when we were drafting the

1 NAI principles for online profiling, we knew what we were
2 talking about. And unfortunately, I think what we've
3 seen on the panel so far today is that largely we don't.
4 And that work needs to happen first. We need to
5 understand exactly what it is that we want to wrap our
6 arms around and then go forward from there.

7 But that definitional work, that definition
8 work really needs to occur first. So I think it is
9 different. I think it's early or premature for us to be
10 able to sit down and write best practices today without
11 really knowing what we're talking about.

12 MR. POLONETSKY: I'd comment on a couple of
13 different levels, one on the comparison to some of the
14 other self-regulatory processes. I think one of the
15 reasons why on the network advertising initiative side of
16 the world things end up working is you could really could
17 sit most of the relevant players who were doing this on
18 any scale around the table.

19 They all were public or soon-to-be public
20 companies that were, you know, part of the civil debate
21 part of the world, and you could say to them, look, you
22 all need to do an awful lot more to explain your business
23 practices, because people have concerns about them. So
24 step up, do more, work harder, bother your customers,
25 make them do more. And since you all are interrelated

1 and your advertisers and your publishers are
2 interrelated, we know that by working with the seven of
3 you, thousands and thousands of web sites are going to
4 have a very different privacy policy or a better notice
5 about cookies and an opt out and so forth.

6 And I think that part is going to be relevant
7 to a certain piece of the industry, you know, that you
8 can see and find, and they'll sit in a room, and they
9 come to FTC hearings, and you know, they want to have
10 their business model work. And, you know, maybe the
11 pressure one way or another way is going to help change
12 either how they do their business or their disclosures.
13 And I'm optimistic that there can be success there.

14 The other big challenge is, however, you know,
15 like in the spam world, is that there is a huge and
16 widespread audience that isn't going to step foot in this
17 room or maybe, you know, anywhere near us. And there the
18 civil, the criminal, all the other technical enforcement
19 measures that are out there are frankly going to be
20 necessary.

21 And the challenge is that you can usually, you
22 know, figure out who's who, and the challenge in this
23 world is you can't always yet figure out who's who. You
24 could figure out who's who if you were there when the
25 software was installed, but you're not always there when

1 the software was installed. And there are companies that
2 were bad guys, and now they're good guys. Or they're
3 good guys in some cases, but they're still bad guys in
4 other cases. And we don't have as clear an audience of
5 let's get the law abiding citizens to be better about
6 littering and picking up and, you know, nicer about how
7 they conduct themselves, and then people who really are,
8 you know, running around with dangerous weapons, you
9 know, wreaking havoc.

10 And unfortunately, they're sometimes wearing
11 the same color uniforms. And so, you know, you're at
12 risk of either technically being overinclusive in a way
13 that frankly solves the problem but is going to need
14 refinement.

15 So I think that's a little bit of a contrast
16 with the NAI and why I think we can probably solve a
17 chunk of the problem with best practices but are going to
18 need a little bit more effective a tool to solve the
19 truly nefarious part of the problem.

20 Just a short comment on the education piece,
21 because I answered that in a long way. You know, the
22 challenge again is, you know, let me go back to the
23 computer guy's mother. There are people who want an
24 education. All of us here who are, you know, are
25 reasonably sophisticated whether we're very technical or

1 not. And we want to know. Tell me a little bit more,
2 because, frankly, I want to know. I don't want to become
3 a mechanic, you know, but I do want to know what the red
4 warning lights mean. Does that mean the car is going to
5 blow up or does that mean, okay, the oil is low, I'd
6 better check it out at some point?

7 You know, kind of -- that's where a lot of us
8 lay folks are. And so we need to educate those folks in
9 a certain way. Here's the tool. Here's what you can
10 buy. Here's what's free. Here's what you can do. And
11 then there's my mother and the computer guy's mom, and
12 they want to know which button to push to make it stop.
13 And so the challenge is giving them that button in a way
14 that isn't too broad, isn't too small, solves their
15 problem in a way that's reasonable for everybody.

16 COMMISSIONER THOMPSON: Andrew, I know you have
17 a response here. But I notice that one of the things
18 Hugh and Brian are sort of in a position that if I listen
19 to Trevor, I was wondering, how long are we going to wait
20 to get a definition before we decide what a best practice
21 is, et cetera, et cetera? You guys are running a
22 business. You have to do something now, because your
23 customers are going to go away. So are you both thinking
24 about this differently?

25 MR. McLAUGHLIN: I actually think we're

1 probably a little bit less allergic to, you know,
2 regulatory, legislative and other efforts in this arena.
3 I got the --although I share a lot of the same fears and
4 anxieties that everybody else does, but I think we're
5 slightly less allergic.

6 It's really costing us money. You know, it
7 costs us revenue. It's costing us goodwill from
8 customers. It causes us to have to use customer support
9 people to answer all these e-mails, give people uninstall
10 instructions, or techies have to try to trace where this
11 stuff is coming from. It's a real burden. We'd actually
12 like to see something happen.

13 But let me say one thing, which is that I think
14 the danger, especially in legislation, of doing something
15 wrong rather than doing something late, is pretty
16 serious. And let me give you just one very specific
17 example. In a bill that was introduced by Senators
18 Burns, Wyden and Boxer, a lot of good stuff in that bill.
19 And I don't want anybody to take this as me trashing it.
20 I think there's a lot of perfectly good work that went
21 into that.

22 One area, though, that is less than ideal and
23 may be harmful is that it says -- it defines as spyware
24 anything that exports network information from your
25 computer, and it includes the IP address, an IP address

1 in that definition. That means that everything that
2 sends a packet from your computer is by definition
3 something that is subject to the notice and consent
4 regime in the bill.

5 Well, on one level, that's perfectly fine. But
6 as a practical reality what that's going to mean is that
7 every application on your computer is going to have you
8 go through a notice and consent scheme for just sending
9 packets. And that threatens to routinize the process of
10 notice and consent so dramatically that the really bad
11 stuff isn't being elevated to the attention of the user
12 in the way that it ought to be.

13 So my point here is this. There are all kinds
14 of I think negative things that could happen through
15 legislation, but what this has kind of driven me back to
16 in my couple of months at Google -- I joined in February,
17 and I was told right when I got there, make spyware a big
18 priority. Go to Washington and figure out what anybody's
19 doing, and let's figure, you know, it's a real problem
20 for us, and see what can happen.

21 The more that I've looked at the text of these
22 bills that have been floating around, the more kind of
23 nervous and worried I've become because they do seem to,
24 you know, hold these second order consequences. And it
25 led me to this conclusion. Even if we had a perfect law,

1 even if the one that I draft on my laptop tomorrow were
2 to be enacted and signed by the President, it's not going
3 to do us a lot of good, right. This is a tool that you
4 can use to go after some providers.

5 But let's be honest. The really bad people,
6 the ones who are responsible for the software I threw up
7 on the slide before, are not going to be dissuaded by a
8 law in the United States that might potentially subject
9 them to liability here. They're not located here, right.
10 They operate in other places, and we're dealing with a
11 global Internet.

12 So this takes me back to just sort of echo
13 something I think John said better than I could earlier,
14 which is that ultimately, just like in the case with
15 viruses, you don't look to the law to stop -- to really
16 protect you from viruses. It has some tools that you can
17 use as a company to go after people. But really, it's
18 technology. It's my Norton anti-virus application that
19 protects my laptop from viruses, not the law.

20 So, you know, I would love to see something.
21 The sooner we can get it together, the better. The
22 sooner we can get best practices together, the better.
23 I'm all in favor of that. I'd like to see some urgency
24 to that. But it does not substitute for the fact that we
25 need to address this problem first and foremost with

1 better technology, better tools, user education, all the
2 things that have been referenced on this panel.

3 I do want to say, though, that because we're a
4 little bit less allergic to that stuff, I hope people
5 will grasp the sense of urgency that we have. And I
6 think one of the things we've got to flag is that there
7 are bills proliferating in the states, and unless the
8 industry is seen to be getting its act together and
9 giving users better tools, we're going to see bills that
10 make people's lives harder rather than easier coming out
11 of the states.

12 MR. ARBOGAST: Obviously, I feel like
13 technology has a huge role to play, but I also am bullish
14 on the idea of defining best practices in the industry.
15 And I'd like to point to the work that Ari Schwartz and
16 folks at CDT have driven in recent months.

17 What we found is it's easiest to identify what
18 is clearly bad. And so I think you'll see first and
19 foremost a consensus of what the really bad stuff is
20 that's clearly deceptive. And to be honest, I think a
21 lot of the laws on the books already make enforcement
22 actions against the worst stuff possible.

23 And I think it's going to take a little bit
24 more time, but it's still very doable to start to define
25 what best practices look like. And then I think concepts

1 like, you know, communities rating software and consumers
2 making use of those ratings are clear opportunities for
3 us in this space. And so I think that technology will
4 move ahead and will help and has to, but I also think
5 that the industry is already kind of moving on the best
6 practices front.

7 COMMISSIONER THOMPSON: Thank you. We have a
8 few more minutes, and I have a series of questions here,
9 some I hope the audience won't mind if I sort of condense
10 and kind of paraphrase, because they revolve around
11 certain kinds of subjects.

12 One, there are couple of questions that deal
13 with a concern that people have about developing best
14 practices and the concept of profit in the sense that how
15 can we be sure that in the industry, and as the industry
16 begins to look at best practices, that it will actually
17 provide customers with choice and not sort of steer
18 people to who they can get financial advantage from, or
19 at least ensure that there is at least some
20 competitiveness there so that one company or another
21 doesn't wind up picking winners and losers?

22 MR. SCHWARZ: Let me jump in just to start.
23 The reason I'd feel that this is not a particular danger
24 is that it has not happened so far. There has been ample
25 opportunity for some company to evolve to be the law-

1 giving single source, all fount of knowledge here, and it
2 has not happened. Even Microsoft with their dominance in
3 the marketplace have not succeeded in providing all of
4 the technology necessary to be on the Internet and to use
5 the Internet.

6 And so I don't think this is likely to happen
7 in this particular domain either. What we do need to
8 make sure, though, is that we have a set of standards
9 that make the use of technology or use of these rules or
10 use of the best practices as ubiquitous as possible and
11 make those standards reasonably open so that no single
12 company can hijack those, if you will, if that's the
13 right word.

14 But I have no fear sitting here today with 25
15 years of experience in this world that this is likely to
16 be a one company take all and the rest of the world is
17 going to go scratching in the dust.

18 MS. MAIER: I think John makes a very good
19 point. I think that one of the first things that any
20 group of organizations trying to do something is to be
21 very transparent and open about their process -- who's
22 involved, what the rules are and so on.

23 I think that all of us when we think about
24 putting together best practices want to do it in a way
25 that we involve not only other industry players but

1 actually specific parts of the industry, so people from
2 operating systems, groups from security, groups from
3 anti-spyware technology, a wide range of industry, not
4 just one player, and involve consumer-oriented
5 individuals, representatives of consumers, and maybe even
6 do some research so that we really are listening to what
7 consumers have to say.

8 But I think if you get enough different kinds
9 of groups that you have wide representation of nonprofit
10 and consumer-oriented groups, and that you keep the
11 process transparent, and obviously work with the FTC to
12 get feedback, I think we'd be better off. I don't think
13 there's a danger.

14 COMMISSIONER THOMPSON: I have another question
15 here. It's a question that notes that there's been a
16 lengthy history of consumer education on such topics as
17 viruses and the use of anti-virus applications that what
18 makes you think that spyware education would be more
19 successful? And I would add a little something to that
20 question which is, and if you think it could be, what do
21 you think we would have to do to make it more successful?

22 MS. MAIER: Start with the kids. You know,
23 just what idea is -- I brought my son here, and at risk
24 of embarrassing him, he's the one who runs the PC. He's
25 the one who puts the spyware on, and he's the one who's

1 trying to take it off.

2 (Laughter.)

3 MR. POLONETSKY: I guess I'd like to give an
4 example from some recent experience. You know, we
5 started talking about reducing pop-ups for our members,
6 and we did, and people continued to complain because they
7 were getting these pop-ups. And of course they ended up
8 being, you know, those Windows messenger pop-ups that
9 spammers were using to send, you know, system messages
10 that popped up, you know, either selling anti-pop-up
11 software, as you know, was referenced earlier, or, you
12 know, just sort of a new kind of spam.

13 And so we said all right, let's tell people
14 what this is; that it's not a pop-up, and that they can,
15 you know, turn it off. And we'll even give them a script
16 that they can click on. And, you know, pretty powerful
17 message. They didn't like it. They didn't want it. You
18 know, click here if you're still seeing a different kind
19 of pop-up and, you know, we'll make it go away from you.

20 And, you know, a lot of people did and a lot of
21 people didn't but kept calling in and costing an awful
22 lot of money, being very unhappy about their experience
23 and costing us an awful lot of money complaining about
24 what was happening to their computer.

25 And so we said, you know what? Why don't we

1 just turn this thing off? Why don't we just push out a
2 script and sort of turn it off for everybody? Tell them
3 we've done so and they're a little healthier because of
4 it. And if for some reason they really want this thing
5 on because they're on a network and it's being used and
6 forth, well then they can turn it back on.

7 But what I think I learned from this and others
8 at the company as well is you've got to do that
9 education, because there are some people who really, you
10 know, don't mess with their settings. They want to tweak
11 everything. And don't do anything. And then there are
12 others where it may be appropriate to say, this truly is
13 good for you. Nobody would argue with whether this good
14 for your health. I'm not, you know, marketing to you.
15 I'm turning this off. So just click the button to say,
16 you know, don't help me today because I can cross the
17 street myself.

18 So I think when we talk about this education,
19 it's got to be, well, let's educate, but it's also, you
20 know, get some consensus about what it's fair to say,
21 sorry, but that's not anything that any reasonable person
22 would want. And if they do, then, fine, let them go
23 ahead and really specifically come back at it.

24 So it needs to be education with a little bit
25 of a push perhaps.

1 COMMISSIONER THOMPSON: Do you agree with that,
2 Brian?

3 MR. ARBOGAST: I think that clearly having
4 smart defaults is definitely one of the things we can do
5 to make it easier for people to protect themselves. But
6 in the end, it is going to come down to customers making
7 choices, and you want them to be informed choices.

8 So giving them the tools so that they're having
9 the help to make an informed choice at the time that
10 something's trying to be installed on their machine,
11 that's the place where we can really make improvements.
12 And that's one of the places where we've focused.

13 COMMISSIONER THOMPSON: Chris?

14 MR. KELLY: I think that process counsels
15 towards a more expeditious and open process in the way
16 that Fran has described to get to definitions on what are
17 the really bad things that we're trying to target here
18 and to separate the bad actors from the, you know, decent
19 client software actors.

20 And, you know, I do applaud some of the work
21 that CDT has done on this already and a number of other
22 groups who are beginning to engage on it. And we need to
23 move that process along as fast as we can.

24 COMMISSIONER THOMPSON: Thank you.

25 MR. SCHWARZ: Let me just add one other

1 thought. I had kind of given you a glass is half empty
2 story up front. Let me give you a glass is half full
3 story at the end.

4 Yes, we have 400-odd million users that have
5 not taken up the anti-virus or anti-attack software. But
6 we have 400 million users that have. And I think we can
7 build on that base with judicious standards, with good
8 approaches, with best practices, with constant perhaps
9 push beyond what we have done so far. It is doable.

10 COMMISSIONER THOMPSON: Thank you. I notice
11 that we're running out of time here, and I'm going to
12 take this opportunity not only to thank you all, but also
13 to say this. You know, those who are involved in the
14 public policy side in the end are accountable no matter
15 what. And you are too in the same position, because if
16 people -- if they have a concern about spyware and they
17 ask us, even if it's a misplaced concern or a concern
18 that's not fully knowledgeable, they expect some action
19 from us.

20 We will need something else to point people to.
21 We will need to show what else is happening out there,
22 how they can find resources to learn more and give
23 consumers choices about what their experience is going to
24 be online.

25 At the same time, you have many of those same

1 pressures, because even though you're not elected, they
2 elect you every day when they decide whether to buy or
3 not to buy or to participate or not to participate. And
4 that's where we have the same challenge.

5 So I would say that we have an opportunity here
6 because we're still early in the process. But the public
7 perception is moving very quickly. So I would ask you to
8 take that into account.

9 So thank you very much for coming, and we
10 appreciate your participation.

11 (Applause.)

12 MR. PAHL: Thank you, Commissioner Thompson,
13 and members of the Industry Response panel. We'll take a
14 15-minute break and begin again at quarter to 4:00.

15 (A brief recess was taken.)

16 MR. PAHL: If people could please take their
17 seats, we'd like to begin in a minute or two. Thank you,
18 everyone. We're about to begin our fifth panel of today,
19 and the fifth panel will address technological responses
20 to spyware. The moderator of this panel will be Beverly
21 Thomas, who is an attorney in our Division of Advertising
22 Practices here at the Federal Trade Commission.

23 Beverly?

24 MS. THOMAS: Thank you. I'd like to welcome
25 the panel today and give them a big thank you. They

1 spent an awful lot of time helping educate me and prepare
2 me for this panel. And I will introduce them, starting
3 again to my left, Steve Bellovin, who is a member of the
4 National Academy of Engineering an AT&T Fellow with AT&T
5 Labs-Research. He also is co-director of the security
6 area of the Internet Engineering Task Force.

7 He co-authored one of the first books on
8 firewalls in 1994 called "Firewalls and Internet
9 Security: Repelling the Wily Hacker", which was
10 substantial rewritten and reissued just last year.

11 Jeffrey Friedberg is next. And he's Director
12 of Windows Privacy from Microsoft. As such, he is
13 responsible for improving the privacy experience for
14 Windows users and identifying best practices for software
15 development.

16 We then have David Moll, who is CEO of WebRoot,
17 maker of the SpySweeper anti-spyware program.

18 Then is Wayne Porter, who is co-founder and
19 primary editor for SpywareGuide.com, which distributes
20 free and paid versions of an anti-spyware program called
21 X-Cleaner, and also serves at the research center for
22 specific spyware programs. He has also been active in
23 efforts to establish a code of conduct for online
24 affiliate marketers.

25 Then we have Danny Weitzner, who is a principal

1 research scientist at MIT's Computer Science and
2 Artificial Intelligence Lab, and he's also a director of
3 the World Wide Web Consortium's technology and society
4 activities. He was the prime mover behind the
5 development of P3P, an automated mechanism for analyzing
6 website privacy policies.

7 This panel will discuss possible technological
8 responses to spyware starting with the tools available at
9 the desktop, then moving up to the network and ISP level,
10 and then moving on to possible big picture changes and
11 developments that could possibly be designed.

12 I think it's going to be a lively discussion
13 because we have a bunch of techs, and techs love to talk
14 tech, so. Before we start, though, because a lot of
15 spyware is often stealthily installed from web pages,
16 I've asked Jeffrey to explain how the download process is
17 supposed to work, how spyware distributors misuse this
18 process, and some changes that Microsoft is planning on
19 making to reduce the inadvertent installation of spyware.

20 MR. FRIEDBERG: If we can have the slides up.
21 They're there. So, as Bev suggested, it might be good
22 just to take a quick review of how this stuff is supposed
23 to look and then kind of go over some of the tricks and
24 some of the new things that are coming down the path here
25 with respect to updates to software.

1 (Slide.)

2 So here's your typical web page. This is just
3 a simulation. It might be a news site that you like
4 going to. And on this page there's some link down at the
5 bottom that says, hey, here's something really cool for
6 you to download. And it might be for something like a
7 cool stock ticker. So you'll click on that thing, and
8 you get the security warning.

9 Now the security warning comes up, and it tells
10 you a couple of things. It says do you want to install
11 and run, and the name of the software, in this case some
12 ticker program. It tells you the name of the publisher,
13 and then you have a choice of yes or no whether you want
14 to do this.

15 Now you're going to get this kind of dialogue
16 anytime you download something that could potentially run
17 on your system. For example, just a general software
18 program or executable, or something they call an ActiveX
19 control. Now ActiveX control, as you may have heard them
20 used a couple of times during the other panels, ActiveX
21 is a plug-in to the Internet browser that extends its
22 functionality. Its sole purpose in life is to add new
23 capability, like, for example, better drawing. Flash is
24 a plug-in that you might have encountered in the past.

25 So it's -- this kind of experience of needing

1 an ActiveX control or whatever or some additional
2 software is pretty common.

3 (Slide.)

4 Now some of the common tricks that we've seen,
5 you know, and they start from just simply confusing
6 things to more misleading things to deceptive things, and
7 I'll go over just a couple.

8 Here's a case of that same security warning,
9 and one of the things you'll notice is that instead of a
10 simple software name, we have suddenly a four or five
11 line software name. I'll just read a little bit about
12 it. It says, "After accepting our license agreements,
13 program one, program two, two free ad-supported downloads
14 that display (1) useful information and (2) branded ad
15 selected based on web sites you view?"

16 Oh, that was a question.

17 "Click here to read our agreements. Click yes
18 to accept."

19 Well, how many more questions will be I asked
20 in one little space? Clearly, this was not the way this
21 was designed. It's designed for a simple name of a piece
22 of software, and some vendors have felt that they could
23 put their entire end-user license agreement here. And
24 clearly, this is confusing.

25 I mean, if you actually read it very carefully,

1 the logic is correct. And if you do click on the yes
2 button at the bottom, it says you've agreed to all our
3 agreements that you actually haven't looked at. Now
4 whether this is legally binding or not is left to the
5 lawyers. But clearly, this is confusing at a minimum,
6 and I would dare say this is not a best practice.

7 (Slide.)

8 So there's another situation that comes up
9 sometimes. It's called the pop under exploit. And here
10 again, you go to that same news site, and you're looking
11 at for a while, and then all of a sudden, that security
12 warning pops up. And you say, you know what? Maybe this
13 for this web page, and so I trust this web page, and
14 therefore I might trust this download, so I might click
15 yes; I might not.

16 But what you don't realize when you look at the
17 screen, underneath there's another, you know, page that's
18 actually in this ActiveX control, and it's that page
19 that's actually popping this up. And this is a case of
20 them hoping that they get lucky and that they're going to
21 pop this security warning on top of a page that you
22 trust, thus confusing you.

23 (Slide.)

24 This is one of my favorites. This is where
25 cancel means yes. This has all sorts of interesting

1 elements in it. First off, the title. It says this is a
2 system update. If you read a little bit further it says,
3 no, it's a security update. And if you read even
4 further, it says it's a privacy protection update.

5 Now in all cases, if you were to hit cancel or
6 the little x in the corner, it all means yes. And the
7 way they do this is that this is really an image. This
8 is not a window with boxes in it. This is a picture.
9 Now to a user and to myself, I couldn't tell the
10 difference. But if you actually click anywhere here, you
11 all go -- what I call all roads lead to Rome. You end up
12 going to the site that they want you to go to to then be
13 propositioned further and get a download.

14 (Slide.)

15 Now here's another example of the same thing.
16 It's that window inside the window that says a security
17 alert. Maybe you could see it. It says: Warning. Your
18 computer is being attacked by spyware and adware. And
19 again it presents yes, no, and cancel buttons. And of
20 course, this is really just an image. Click anywhere on
21 that image to make it go away, now you go back to the
22 site and you get entrapped in their little web.

23 And then furthermore, down at the bottom, it
24 says chances of you having adware software installed is
25 99 percent. Now I don't know how they figured that out

1 without really scanning my system, but clearly, you know,
2 this is getting very deceptive here. It's quite
3 misleading. They've provided user interface components
4 that don't work. And I'd say, you know, time to go after
5 these guys.

6 Now my mom had a similar version of this, and
7 no one really mentioned it in the earlier panels, but it
8 was combined with a CD tray opening up and closing. So
9 there she was sitting there, and the CD tray is opening
10 and closing like there's a ghost in the machine.

11 (Laughter.)

12 And up pops the window that says, if you pay us
13 \$35, we can make this go away.

14 (Laughter.)

15 Now I don't know about you, but that sounds a
16 little bit like extortion. And, you know, clearly, it
17 turns out that you can easily open and close the CD tray.
18 It's a normal function of the computer. It has nothing
19 to do with being compromised. And so here they're just
20 trying to instill fear to get you to download the tools
21 that they're trying to sell you.

22 Now my blood is beginning to boil a little bit.

23 (Slide.)

24 Now there is a couple of other ways this can
25 get on your system. One is to accidentally leave your

1 front door open. This is the Internet explorer. These
2 are the options that you actually have, and there's a
3 slider, which is on the left there, that indicates the
4 level of security.

5 Now the default that we set it to is medium,
6 which is a very good place for it to be. Some people may
7 want to even go higher than that. There are some
8 scenarios where you might need to set it lower just maybe
9 temporarily to get a particular download from a
10 particular site that has weird permissions.

11 If you leave it in the low position,
12 unfortunately, you're now exposed to drive-by downloads.
13 This is where a web page says, hey, I've got this ActiveX
14 control. And guess what? When you say low, that has the
15 same meaning as saying I trust all web sites everywhere.
16 And you won't get any dialogues, you won't get any
17 warning. So this is a very dangerous position to leave
18 your setting in. My recommendation is always leave it on
19 medium or better, and if you need to set it to low, do it
20 just temporarily and move it right back.

21 A couple of other things is that, you know, in
22 general, the other ways that you might actually get
23 software on your system is through what we've heard
24 earlier be called security vulnerabilities. Now software
25 systems, as we've been developing them, unfortunately

1 sometimes have security problems, and we've been fixing
2 them and other companies have been fixing their problems,
3 you know, routinely.

4 To avoid getting software through a security
5 vulnerability, we strongly recommend, number one, keeping
6 your software up to date. In this case, I would go to
7 Windows update or turn on automatic updates. Get
8 yourself a great anti-virus program. Make sure that's on
9 and up to date. And these are the kinds of things. And
10 of course, if you have a firewall, turn that on as well.
11 And these are the things that can really help protect you
12 from the things that are doing really malicious attacks
13 through security vulnerabilities.

14 We've also heard in the earlier panels that
15 when you get spyware on your system, they sometimes
16 burrow and create new holes. So as you infect yourself
17 with spyware, you're actually creating little Swiss
18 cheeses out of your system. And, you know, do all the
19 things that I mention, and you start to close this up a
20 little bit, because there's companies that are devoted to
21 trying to find those holes and fill them up.

22 Okay. So it turns out that in our next release
23 of XP, which is coming out in the summer, it's called
24 ServicePak2, there are some enhancements that can
25 actually help address this problem. I'll go over just a

1 couple.

2 Clearly you've all had this experience. You go
3 to a web page, oh, you get the pop-ups, and, yeah,
4 they're for ads and whatever. It's just a common fact
5 that pop-ups will increase your exposure to spyware.
6 You're just being propositioned more often. There could
7 be sites that aren't, you know, fully on the up-and-up,
8 and who knows what they're really offering.

9 So we actually have included a pop-up blocker
10 as part of the base system in IE, and it gives you both
11 notice and choice. There's a new information bar that
12 lies right underneath the address bar at the top where
13 you normally see the path where you're going. And if
14 there's a pop-up or something like that, you'll get a
15 message that says a pop-up was blocked, and to see the
16 pop-up, click here for additional options. And then you
17 get some choices like, you know, look at them, et cetera,
18 or decide to turn off pop-up blocking.

19 The bottom line is, you're in control. You can
20 reduce the amount of times that you're going to be
21 propositioned for things, and that we think is a good
22 thing.

23 Next is what Brian referred to earlier as a
24 blocker for unsolicited downloads. We know that one of
25 the problems is that people are still barraged with, you

1 know, download my piece of software. Those earlier
2 security warnings just popping up.

3 So we've added a blocker for those, and the
4 logic of the blocker is that if you haven't initiated
5 that download, if you haven't clicked on something and
6 the page is just trying to shove this in your face, then
7 it can get suppressed. And it goes again on this
8 information bar that was added, and then you get a chance
9 later to potentially act on it.

10 We believe this is a big advantage, because now
11 your user experience isn't interrupted. For example, if
12 my kids are playing with something and they get this
13 ActiveX experience, you know, or any other executable
14 download experience, I don't have to worry about them
15 accidentally having to say yes to the question. They
16 won't even get the question. It's going to be suppressed
17 until you decide you need to go back and get one of these
18 things.

19 In most cases, the page is going to tell you
20 when it actually needs the particular ActiveX control or
21 you're going to ask for it specifically because there's
22 some cool functionality you want. It's the unsolicited
23 ones that we think we need to stop.

24 (Slide.)

25 So that multi-line security warning I showed

1 you earlier that was confusing, which is on the left,
2 we've redesigned the whole prompt on the right. And
3 you'll notice that it's very clear at the very top it
4 says, hey, do you want to install this software? Well,
5 what software are we talking about here? Well, there's a
6 name field and a publisher. And the name field is a
7 fixed length. It won't go multiple lines.

8 So when someone tries to do something a little
9 tricky, like trying to get their whole end-user license
10 agreement there, it's going to turn to ellipses at the
11 end, and it's going to be pretty obvious that someone's
12 doing a little more than they're supposed to. The
13 publisher is clearly identified.

14 And we've added a new option in this list. If
15 you look at the one on the left, it says always trust
16 content from the publisher. Well, in today's world, I
17 don't think that's the best option anymore. It's
18 unfortunate but true. We now need to have this other
19 option that says never install software from this
20 publisher.

21 So built into the system is a block list which
22 you as a user can control. You know, if you happen to
23 know there's publishers you don't trust, fine. Just say
24 never install, and then you won't be bothered.

25 (Slide.)

1 And then finally, for expert users and for
2 support professionals, there's a new add-on manager for
3 the Internet Explorer. One of the challenges is that,
4 well, what happens if someone did say yes at some point
5 and you got compromised? Well, you'd like to at least go
6 in and see what kind of ActiveX controls are installed or
7 what kind of browser helper objects are installed. The
8 browser helper object is the technology used to build
9 toolbars. SO if you like downloaded the Google toolbar,
10 it would probably show up on this list.

11 But you'll notice there are some on this list
12 that look like magic numbers and stuff you don't
13 recognize. So a support professional could go in there
14 and help figure out what's wrong with your machine. And
15 so this is just one of those extra steps.

16 In addition, once you see these things on the
17 list, you can actually disable them. You could say, you
18 know what? I don't know how this got here, but I'm going
19 to turn this thing off. And people talked earlier about
20 how hard it is to uninstall some of this software, you
21 know, all these registry entries and all these files for
22 1,000, 2,000, et cetera. By going directly to where this
23 would get called, we can actually prevent this from
24 running. We call it neutralization.

25 Instead of actually removing the files, at

1 least it stops running and stops hurting you. And then
2 maybe you can get an anti-spyware tool or some other tool
3 that might go in and clean up all the mess. But at least
4 you'd have some control right now in your own hands.

5 So, to wrap up, the things I just want to leave
6 you with is, you know, definitely secure your system.
7 The other thing is to download carefully since there is a
8 lot of suspicious activity. Keep up-to-date anti-spyware
9 if you can get it. And also I highly encourage people to
10 load the new XP SP2 when it comes out since it has a
11 number of these very nice features to help address this
12 problem.

13 MS. THOMAS: Thank you, Jeffrey. I think those
14 slides were really good in helping us understand what the
15 problem is and some changes that might help on them.

16 I take it from the one that you're actually
17 doing away with the single click download. Is that the
18 ActiveX blocker because it's unsolicited, so you --

19 MR. FRIEDBERG: Well, that particular feature
20 addresses this unsolicited situation?

21 MS. THOMAS: okay,

22 MR. FRIEDBERG: You know, whether we ever get
23 to a place where there's enough trust where one click
24 makes sense, you know, we'll have to see. Users still
25 want simplicity.

1 MS. THOMAS: Right.

2 MR. FRIEDBERG: But, you know, it's hard right
3 now because you don't know who to trust.

4 MS. THOMAS: And then I have another question
5 about these downloads that a web page makes, and I want
6 to ask our very own firewall expert here, if consumers
7 have set up a firewall and they think, why am I getting
8 this stuff? I have my firewall. Why isn't it stopping
9 it?

10 MR. BELLOVIN: Firewalls only look at certain
11 things, certain -- technically speaking, is they look at
12 certain levels of the stack, and they don't look past it.
13 Think of getting a piece of ordinary mail in your mailbox
14 the post office is delivering. Well, you can look at the
15 from address and to address, and that's really all the
16 post office is looking at.

17 Maybe you've got a secretary who's going to go
18 read that piece of mail and decide something, or maybe
19 just sort this department, that department, or another
20 level, understanding what it means. Think of how many
21 ways you can say I love you.

22 Trying to understand all these different things
23 is time consuming, expensive and extremely difficult, and
24 most firewalls don't do it. Firewalls were aimed at
25 particular threats. They try to block specific kinds of

1 things. You could build a firewall to block some of
2 these things, but ActiveX control. Some people want
3 ActiveX controls, and a firewall that blocked all of them
4 would be disabled. It would be getting in your way
5 instead of helping you.

6 So you can't -- it's a help. What I'd like to
7 tell you about firewalls, it's like it says on
8 toothpaste. It's an effective network security device as
9 part of a program of good computer hygiene and regular
10 professional care.

11 (Laughter.)

12 MS. THOMAS: Okay. Okay, I'd like to turn to
13 tools that are available now at the desktop level for
14 users to obtain. And the first are programs that scan
15 and try and detect the spyware that a consumer has
16 already installed on their PC.

17 David and Wayne, I think both of your companies
18 offer such a product. Could you briefly explain how your
19 product detects spyware and what it does with the spyware
20 once it has identified it? And, David, could you go
21 first?

22 MR. MOLL: SpySweeper is one of our WebRoot
23 products, one of 13 today that's aimed at allowing an
24 average PC user a measure of privacy and protection, and
25 we say peace of mind as well.

1 The product is a signature-based product today,
2 largely, although we see that gravitating rather rapidly.
3 That means that it's by its nature reactionary; that we
4 operate off of a signature file that uses spies that we
5 trap in the wild to identify what they look like when
6 they're on your machine, and that helps us quarantine
7 what we find on a PC when we find it.

8 We really think of our product as being user
9 empowerment. We give people a clear stated option on
10 what to do with a piece of spyware, and that includes
11 offering full page-long definitions of what something is,
12 where you might have gotten it, what it can do on your
13 system, and then of course offer you the ability to
14 render it neutral by putting it into your quarantine and
15 ultimately to delete it off of your system.

16 MS. THOMAS: Okay. Wayne?

17 MR. PORTER: Yes. We have two basic
18 strategies. We have what we call the quick scan where we
19 actually target registry keys, class IDs, window titles.
20 We look at a number of specialized routines to get rid of
21 some of these adwares and spywares that are very
22 difficult.

23 And then we are moving -- we're beta testing
24 now what we call DeepScan, which uses a combination of
25 file check sums, which are mathematically secure file

1 properties such as size and hidden attributes as well as
2 signature-based scanning, which lets us scale a lot
3 faster.

4 When we started scanning for these back in late
5 1999, there was only a handful, and it was very easy to
6 craft routines to detect them. Now, I mean, they are
7 literally just flowing into the market like water.

8 The primary difference is we also -- we
9 actually wrote a scanner in ActiveX. We designed it so --
10 -- basically, I was on a trip and I went to a public
11 terminal and I started typing. I thought, you know, I
12 really don't know what's here. So we designed that to be
13 run remotely.

14 MS. THOMAS: So in other words, some of the --
15 like if you went down to Kinko's and wanted to use their
16 computer, you could run your scanner?

17 MR. PORTER: Right. You can run it from
18 wherever you were at as long as you have ActiveX enabled
19 and you're able to use that. And there's actually been
20 cases at Kinko's, you know, where people have installed
21 key loggers, and that's been a big spot for identity
22 theft.

23 MS. THOMAS: You both used the term "signature-
24 based." Would one of you like to take a stab at
25 simplifying that?

1 MR. MOLL: I can give it a shot. Effectively
2 what it does, we create a digital fingerprint from a
3 piece of known spyware, and we compare that to the files
4 on your system.

5 The algorithms that we use to create those
6 fingerprints are certain enough that if we match it, we
7 know we've found something. So it gives us a chance to
8 look at a PC and to know what's good and what's bad on
9 it.

10 The place where things are moving, however,
11 Bev, is really towards what we think of as sharistics.
12 And we've seen these kinds of things happen in many ways;
13 first with anti-virus where AV products were largely
14 signature-based first and now today have moved towards
15 heuristics.

16 We have referenced spam here I think on every
17 panel at some point, and here's our shot now. We've
18 moved from static blacklists for spammers to a heuristic
19 or a means by which we can infer on a piece of spam
20 without knowing its sender that it may in fact be an
21 unsolicited message.

22 So we find that our own spyware research is
23 moving much this way, to identify behaviors and
24 properties that don't require necessarily a file be
25 signaturized before we can identify it.

1 MS. THOMAS: Okay. You both said I think that
2 you bring up a list or quarantine the spyware that you
3 find. Why don't you simply remove it? Why bother the
4 consumer?

5 MR. PORTER: Well, in some cases there's
6 definitely software that the consumer wants, and we want
7 the consumer to be empowered to make the choice. And in
8 some cases, there's contracts that they may have entered
9 into that, you know, we may not -- you know, we don't
10 want to interfere with that contract they have with a
11 third-party software.

12 MS. THOMAS: And this is --

13 MR. WEITZNER: Bev, let me just say --

14 MS. THOMAS: Sure.

15 MR. WEITZNER: That's the perfect answer. But
16 there's a real answer under it too.

17 MS. THOMAS: Okay.

18 MR. WEITZNER: We've been talking about
19 definition and the need or the absence of legislation
20 today, and I think most of us think about the legislation
21 empowering us to go out as a society to find and
22 prosecute people who are operating outside of what we
23 think is good behavior.

24 However, the absence of that legislation also
25 leaves people who are providing the empowering tools

1 today, like us, at risk. And part of the need for
2 definitional structure in this space today is to make
3 sure that the folks who are acting on behalf of consumers
4 and protecting everybody's mom in here apparently, have
5 the opportunity to do that with a mandate.

6 MS. THOMAS: So in other words, rather than you
7 censoring, you just identify what could be considered
8 spyware and let the consumer decide what to do with it?

9 MR. WEITZNER: That's the way it is today, and
10 I think that's right for where we are. But again, the
11 need for definitional context here is absolutely
12 necessary.

13 MR. FRIEDBERG: I'd like to add something to
14 that. You know, as we continue to look at this problem,
15 there's really three different types of information that
16 is very helpful to have. One is deceptive practices,
17 examples of them. And knowing what's bad and everybody
18 agreeing is a wonderful thing, and that's kind of the
19 work that CDT has started and that the FTC is very
20 interested in.

21 At the other extreme, there are the best
22 practices, which we all know is a wonderful thing for
23 industry to adopt itself and to, you know, justify things
24 like self-regulation, et cetera, if they call all be good
25 actors. But what we're sort of missing is what we'll

1 call objective criteria. And this is really what the
2 protection companies need in order to do their business.

3 They need to be able to go in, look at software
4 objectively using some kind of criteria, assess a piece
5 of software, and know they're not going to get a lawsuit
6 when they put somebody on a list. And that's one of the
7 missing pieces. And objective criteria is quite
8 challenging. Each anti-spyware company has their own
9 sort of definition of this, but I don't think there's an
10 industry consensus on what that is.

11 MS. THOMAS: Okay. David and Wayne, just
12 briefly, what are the limitations of scanners?

13 MR. MOLL: Well, I think the first and the most
14 important relates to the fact that there's that necessary
15 lag. You have to have one to know one at that point.

16 So I think that that today is a limitation to
17 the existing scanners. Now that's going to change real
18 quick because we've identified the kinds of things that
19 we think make for workable heuristics, and they're
20 rapidly approaching the marketplace. They'll be out
21 before SP2 I think.

22 So we think that -- let's not confuse scanning
23 I think with probably the desktop or the end-point
24 security, because I think that that's really always going
25 to be an important component of an overarching system or

1 a solution. So desktop needs to be, even in an ISP or a
2 larger network view, an important component of the right
3 solution.

4 MS. THOMAS: Okay. Wayne, I think you also
5 have a product that's an ActiveX blocker, and you
6 mentioned briefly how it works. Do you want to explain
7 about the class ID?

8 MR. PORTER: Yeah. We use the class ID, which
9 is sort of a unique identifier. And this is free. This
10 is a spyware guide. It's free for personal use. And it
11 can be merged right into the registry. And basically we
12 use Microsoft's kill bit functionality, which sort of
13 makes that program incompatible with Windows. So when
14 they try to run it from a web page, it'll kill it. Or if
15 it's already been installed and tries to run, it'll stop
16 their program from running.

17 You know, it's not the perfect solution.
18 There's definitely some limitations. It's more of a
19 stopgap and it sounds like Microsoft with the
20 ServicePak2, they're greatly going to augment that sort
21 of functionality.

22 MS. THOMAS: Okay. I'd like to turn now to
23 possible solutions at the ISP or corporate level.
24 Because the tools we've been talking about right now,
25 it's up to the consumer to go get them. And, you know,

1 some consumers are going to say, now wait a minute. I
2 had to get an anti-virus. I had to go get an anti-spam,
3 and now I've got to go get an anti-spyware. It's just
4 too frustrating.

5 So are there possible solutions that would be
6 more transparent to users and reduce the need for
7 constant computer maintenance efforts by consumers? And
8 one example, would it be possible to filter at the ISP
9 level, maybe using ActiveX block lists or something else?

10 MR. WEITZNER: Can I take a crack at that, Bev?

11 MS. THOMAS: Sure.

12 MR. WEITZNER: We are today a partner of
13 EarthLinks, and their spyware blocker takes the
14 SpySweeper technology and moves it into their total
15 access toolbar.

16 We think that that's a pretty good paradigm for
17 a place to start today. Filtering at the network level I
18 think is very difficult, at least for the moment. That's
19 going to change here over time. But at least the
20 opportunity to have an ISP step up, as AOL, and Jules is
21 going to be out I know with something shortly as well.
22 You can offer the functionality, keep it hosted on the
23 desktop but make sure that for the consumer it's as
24 painless as possible.

25 A tremendous amount of usability work went into

1 our EarthLink solution, as I know has gone into AOL's.
2 The fact that it's paid for with your subscription makes
3 it even easier. I think those kinds of solutions, which
4 we've seen now work for spam, for anti-virus, pop-ups and
5 now spyware, represent the future of what I think will be
6 the solution here from a technological standpoint.

7 With the connection, you have exposure. And as
8 John pointed out on the last pane, 400 out of 800 million
9 to me is very much half empty, because the unprotected
10 perpetuate the problem.

11 So I think the ISP standing up as they have so
12 far represents the future here, and we for one are making
13 sure that they have a good set of tools to do it with.

14 MS. THOMAS: Steve?

15 MR. BELLOVIN: Yes. Let me disagree at least
16 somewhat there. ISPs are a great spot -- point of
17 contact. The software you get from them, because they
18 are the consumer's contact with the Internet, whatever
19 that is. As we've heard repeatedly today, they're the
20 people to whom many consumers turn, the other of course
21 being their host vendor.

22 But you don't want to do too much in the
23 network. For one thing, it slows it down. For another
24 thing, you really run a real danger of stifling
25 innovation. If you're in a situation where the only

1 things you can connect to from your desktop machine are
2 things that your ISP has pronounced safe, we have to
3 remember that the World Wide Web was not designed by
4 ISPs. It was designed by a guy in a physics laboratory
5 in Geneva. And it was possible on the Internet -- made
6 the Internet that we know of today, precisely because the
7 ISPs don't control what you see.

8 So there's a lot of danger. I'm not saying
9 that there's no role for the ISPs, not by any means. I'm
10 saying we've got to be very careful about how it's done
11 and what responsibilities we give the ISP by regulation
12 or statute, for fear of putting them in a position where
13 we really don't want them to be.

14 MS. THOMAS: Danny?

15 MR. WEITZNER: Just quickly. I think that,
16 Beverly, it's important to distinguish different types of
17 what we might generically call ISPs. AOL offers
18 certainly ISP service, but they clearly offer a whole lot
19 more.

20 So it makes some amount of sense for them to
21 say they're presenting you an environment that has
22 certain characteristics that goes well beyond whether the
23 packets flow in and out of your computer correctly. Some
24 people want that. Other people don't. Institutions by
25 and large don't want that, because they want to control

1 the way the packets flow around their institutions.

2 So there may be some degree of solutions from
3 ISPs for certain kinds of environments for people who are
4 paying their ISPs to guarantee a whole lot more about
5 their environment, and others besides AOL do it. But as
6 a generic matter, I agree with Steve certainly as to the
7 web, but also as to the limitation of what the pure
8 provider of Internet access can ever do here.

9 MS. THOMAS: Well, I think what David was
10 saying was that the way theirs works, it alerts people.

11 MR. WEITZNER: Right.

12 MS. THOMAS: To this is what you've got.

13 MR. WEITZNER: Yes.

14 MS. THOMAS: What do you want to do?

15 MR. WEITZNER: And that's clearly EarthLink
16 offering a value-added service to their customers that's
17 presumably going to make their service more attractive.
18 So that's certainly a good thing. And hopefully --

19 MR. MOLL: Well, and given that the societal
20 cost is being borne out in large part by the ISP who
21 today takes the phone call, I think we can't blame them
22 nor can we fight that tide that they're going to adopt
23 solutions.

24 MR. FRIEDBERG: I would just like to point one
25 other thing out. That as we learned earlier today, this

1 whole spywares base is quite a continuum, and there's bad
2 stuff at one end and there's kind of grayer stuff towards
3 the other end.

4 And, you know, quite frankly, I don't want
5 someone making a decision for me whether or not a piece
6 of badware is in my best interest or not. Maybe it's
7 going to save me 120 bucks a year on a subscription, and
8 that's perfectly okay with me.

9 So I don't know what policies are going to be
10 put on at the ISP level. Clearly, I'd like them to stop
11 the bad stuff. But, you know, once you get into that
12 gray area, it gets a little tricky.

13 MS. THOMAS: What about corporates,
14 corporations putting filters on their network?
15 Different? Is that different?

16 MR. MOLL: I think it's equally essential, in
17 fact perhaps more so. When we think about some of the
18 things that we've talked a little bit about, key loggers
19 and Trojans, you know, at the individual level we call
20 that identity theft. But at the corporate level, that
21 has the potential to be very serious fraud.

22 What happens when a payroll clerk gets that
23 Trojan or when an accounts payable clerk gets the key
24 logger? The potential here for harm is just simply much
25 bigger. And in fact, I would speculate that one of the

1 trends we're going to see is that now they've figured out
2 a few tricks in the spyware game, they're going to go for
3 bigger fish. And it's not my Visa that they're going to
4 hit. It's going to be Fidelity or Bank of America or
5 somebody that's real scale.

6 So, we again are trying to architect solutions
7 that are appropriate for those places. The consumer is
8 still the end game here, because it's so much of our
9 personal, financial or medical data that can be lost even
10 in the corporate environment.

11 So I think that the problems here are just
12 simply going to be bigger and more important.

13 MS. THOMAS: Okay. I'd like to move on to the
14 big picture, possible tools that we might be able to
15 develop, and I'd like to start with a P3P-like tool. And
16 Danny, could you start by explaining briefly what P3P is
17 and how it works in assessing website's privacy policies
18 and then address whether something similar could be
19 developed for spyware?

20 MR. WEITZNER: Sure. For those of you who
21 don't know, P3P is the platform for privacy preferences.
22 It's a set of technical standards deployed on the web.
23 It's implemented in web browsers, on web servers by
24 people who produce web sites, and it's basically designed
25 to do one thing. It's designed to enable users of the

1 web to make informed choices about what kind of privacy
2 relationships they enter into.

3 I'm going to spare you a lot of the technical
4 details because time is short. But the key motivation
5 for P3P was a recognition quite some time ago that
6 actually came out of some of the early FTC online privacy
7 workshops, that it's awfully hard for people, for average
8 consumers, even not average consumers, to read privacy
9 policies. And in fact, I would say, to the extent that
10 that was true in 1996 or '97, it's probably all that much
11 harder today.

12 We heard about the complexity of different
13 pieces of software interacting on computers. We're well
14 aware of the complexity of interacting privacy policies.
15 You give your information to one place. It goes
16 somewhere else as part of a perfectly legitimate business
17 relationship, but you try to disentangle that through the
18 10-page privacy policy from the first website you visited
19 and the 15-page policy that is on the site of the partner
20 that you might or might not have visited, and pretty soon
21 you get consumers who throw up their hands.

22 We want to try to make that simpler, to enable
23 people who collect data to express their privacy policies
24 in simple, machine-readable terms, and then enable users
25 to establish what their privacy preferences are and rely

1 on their browsers or other pieces of software they use to
2 help make decisions about whether the privacy
3 relationship they're being asked to agree to is one that
4 they're happy with or not, based on what their general
5 preferences are.

6 Now I think that the key feature of P3P really
7 was a particular kind of transparency. It was what I
8 would call an active transparency. So it's not just
9 having notice, but actually being able to act on the
10 notice you get in a way that's clear and simple, and I
11 think most importantly, doesn't take up too much of the
12 user's time.

13 It's been very clear to all of us who have
14 worked in this area that people really don't want to put
15 a whole lot of time into these problems, into -- frankly,
16 into managing their privacy relationships, into managing
17 their spyware. People don't come to their computers to
18 protect their privacy. They don't come to their
19 computers to get rid of spyware. They come to their
20 computers to send e-mail or write a document or do
21 whatever they're doing.

22 And to the extent that you impose added costs,
23 even with the best education programs, people simply will
24 frankly not protect themselves very often. And when
25 enough of that lack of protection happens, we have the

1 sort of network effects of problems that have been
2 described here.

3 So the critical question, can this sort of
4 approach work or help with the spyware problem? Very
5 clearly, in the case of privacy, P3P only has helped in
6 the privacy arena as part of a much larger view of the
7 privacy question.

8 Just to take a U.S.-centric perspective for the
9 moment, the FTC and others made it very clear that they
10 expected, with or without law, with or without new law,
11 that web sites would have privacy policies. They did
12 that. Then you could start to put those privacy policies
13 into P3P terms and people could start to make decisions
14 based on that.

15 So you've got a -- we clearly have to think of
16 this as part of a much larger question than whether
17 there's a piece of technology, whether it's the anti-
18 spyware technologies or whether it's some kind of
19 labeling system like P3P, there will have to be a much
20 larger approach. The NAI and Trustee are examples of
21 other layers that you have to consider in the case of
22 privacy, and I would say the same thing would have to be
23 true in the case of spyware.

24 I have to say, I'm slightly on the fence here
25 about how much a labeling approach can really accomplish

1 when it comes to spyware. And I think it can probably
2 help some, but the history of trying to label things on
3 the web I think is really instructive here. I think if
4 you look at both privacy on the one hand and things like
5 pornography and spam on the other hand, you see the sort
6 of limits and benefits of labeling.

7 In the case of privacy, labeling clearly helped
8 because for the most part, you had people who were
9 collecting sites, that were collecting personal
10 information. The legitimate ones had privacy practices
11 that were bona fide statements of their actual privacy
12 practices. And then people could make choices based on
13 those statements. To the extent that spyware fits into
14 that sort of category, that's great.

15 On the other hand, you have spam, where clearly
16 spammers for the most part don't have a particularly big
17 interest in labeling their spam as spam, and hence, all
18 the problems that we have with spam. So you've seen with
19 spam that the solutions tend to come in other parts of
20 the network and frankly don't tend to rely too much on
21 the good faith behavior of the spammers. What the
22 solutions certainly do is they try to make it more
23 expensive to be a spammer and make it harder to be a
24 spammer.

25 So I think that's going to be an important part

1 of the solution here, and for better or for worse, that
2 just doesn't have a lot to do with labeling.

3 As Jeffrey said, though, there is clearly a
4 very substantial gray area of applications that might be
5 downloaded onto a person's computer or run somewhere on
6 the web in relation to that person's computer. And I
7 think it's in that gray area that a labeling approach can
8 really help a lot.

9 I think that clearly what's happening is that
10 whether it's from a residential sort of consumer level
11 ISPs like EarthLink and AOL, or through private end-user
12 products, people are going to be putting up walls to
13 spyware because they have to. And I actually am worried
14 in many ways about the effect that that can have on
15 innovation.

16 As it happens, some of the first P3P-enabled
17 pieces of software, software that enabled people to read
18 P3P policies, were plug-ins and ActiveX components, and
19 they might well have been blocked by some of you
20 gentlemen's spyware products with all the best intention.

21 So I think that it's going to be very important
22 for the legitimate providers of downloadable applications
23 to have some way of identifying what their applications
24 do and enable people to make choices. Maybe people will
25 say, don't download anything that doesn't have that kind

1 of label on it, so that I can make a choice. And then
2 within that, they'll say I'm willing to download things
3 that have certain functions but not others.

4 I think that operating system vendors and
5 browser vendors can help an awful lot in working,
6 developing best practices, developing a taxonomy of
7 functions of applications that are downloaded and enable
8 people to make better choices.

9 No one up on any of these panels today is able
10 to make all these choices for a user. We have to give
11 users the ability to distinguish in that gray area of
12 things that are legal but maybe wanted, maybe not.

13 MS. THOMAS: I think that Steve had some
14 thoughts on that?

15 MR. BELLOVIN: I'll make one comment. Labeling
16 will work a lot better if it's something the operating
17 system can enforce. For example, a plug-in that wants to
18 see what URL you've just gone to, if the operating system
19 can make sure that the only way to get to the URL is if
20 the application has said this is what I want to do and
21 the user has consented, and the operating system is
22 sufficiently locked down that there's no way around it.

23 Figuring out the set of possible actions, the
24 vocabulary is hard. Figuring how to lock things down is
25 really hard, and I doubt that any operating system today

1 can do it. Have to depend on you guys to lock it down
2 enough to make sure that we got the right interfaces
3 present.

4 MS. THOMAS: Okay. I'd like to -- go ahead.

5 MR. FRIEDBERG: I just want to make one last
6 comment. You know, I'm very encouraged by the prospect
7 of best practices if we can more or less pursue those.
8 And I really would like to see companies rewarded for
9 doing and following best practices, and sometimes you may
10 need a seal of some kind of a logo program to know very
11 quickly whether they're following these practices.

12 But I know I would direct my own personal
13 commerce toward sites and things of that nature and other
14 applications that had the right seal on it.

15 MS. THOMAS: Well, I'm wondering. The security
16 alert, the new one that you designed, that said always
17 trust this one, could you set that only for those who are
18 -- you know, if it's somebody who's following best
19 practices, you could say, okay?

20 MR. FRIEDBERG: This is all possible once we
21 establish the best practices and figure out what the
22 certification programs are.

23 MR. WEITZNER: I'm going to just make one
24 suggestion. I think that best practices are great if
25 they describe a set of practices among which application

1 writers and users can choose.

2 I think that it would be unfortunate even if a
3 diverse group, an open group, got together and said here
4 are the things we'll allow; here are the things we won't
5 allow. And I don't think you're suggesting that,
6 Jeffrey, but just to be clear. Best practices doesn't
7 mean a single list of the good things and the bad things.

8 Best practices I think means doing the sort of
9 thing that the now much-mentioned CDT report -- it should
10 have been on Amazon. It would have done really well
11 today -- would identify a set of problematic behaviors
12 and could identify a set of other behaviors and then let
13 people make choices.

14 MS. THOMAS: Right.

15 MR. FRIEDBERG: Let me just clarify. On the
16 best practices, I also see that as a continuum. And on
17 one end there's sort of a minimum bar or a minimum level
18 where you have to be legitimate, and that means you have
19 to follow all the laws and not do anything illegal. You
20 should be okay to go at that point.

21 Then there's the other extreme where you're
22 doing some really extraordinary things that users really,
23 really like. And to some extent, you should get gold
24 stars when you do stuff like that. It's more
25 aspirational, and may be optional, and may be more

1 expensive for some companies to do than others.

2 So you need enough latitude in the best
3 practices so that, you know, the full spectrum of
4 legitimate applications could get developed, and those
5 that have the energy and resources actually can do even a
6 better job and be rewarded in the marketplace.

7 MS. THOMAS: Okay. I'd like to move to another
8 idea that I think, Steve, you brought up. Would setting
9 up separate lockboxes for individual programs -- i.e.,
10 requiring programs to only run in their own compartment -
11 - help reduce the problems in spyware, particularly
12 browser hijacking or co-opting a consumer's computer for
13 its own purposes?

14 MR. BELLOVIN: It is a good idea. Again, it's
15 still in the research stage. You sometimes call them
16 sandboxes or lockboxes. Make sure that there's a limit
17 to what certain programs can do enforced by the operating
18 system. It ties in again with the labeling question.
19 You know what it can do and what it can't.

20 The trick is to retain the usability of the
21 system while you're doing that. The minor part is the
22 fact you've got to redesign all your browsers and mailers
23 and so on. The hard part's making the system usable.
24 Look, I'm a Unix user, so I have a very warped notion of
25 what user-friendly is.

1 (Laughter.)

2 But, you know, I recognize there are a lot of
3 challenges there.

4 MS. THOMAS: Jeffrey?

5 MR. FRIEDBERG: I think sandboxing that kind of
6 strategy is actually very interesting and we should
7 continue to look at it to see if we can get our arms
8 around it and see if there's a way to define a ring of
9 well-defined behavior that's quote/unquote "safe" or if
10 something were to run in the sandbox it can't -- the mess
11 is going to end up only being in the sandbox, not hurt
12 anything else. That's kind of the strategy.

13 One of the things that we've realized -- just
14 to finish -- is that, you know, most programs, although
15 they can live in the sandbox, want to go a little bit
16 beyond it. And as soon as you have one or two features
17 that they want to do outside the sandbox, imagine needing
18 to engage a customer saying, oh, you know, it's perfectly
19 safe. It's doing the sandbox, but also wants to use port
20 25. Is that okay? I don't know how to make that trust
21 decision as a user. And so while the technology may be
22 there to form a sandbox, we still haven't figured out how
23 to translate that into meaningful decisions for users.

24 MS. THOMAS: Okay.

25 MR. WEITZNER: You know, I think there's

1 sandboxing programs and then there's sandboxing users,
2 Jeffrey, I think is where you're heading.

3 People don't want to be sandboxed. I mean, the
4 great thing about computers is that you may say, you
5 know, on 364 days of the year, you do want to sandbox
6 your personal financial data from your e-mail program.
7 It may be on the 365th day you want to send some person,
8 maybe it's your accountant, all your financial
9 information. And there goes your sandbox.

10 So I think a more -- a labeling approach that
11 is more based on the functionality as opposed the way
12 programmers happen to write programs would -- is probably
13 going to be required here. Because otherwise, people
14 will just turn it all off and say forget the sandboxes.
15 They're too --

16 MR. MOLL: Well, I think there are shades of
17 gray even here. I mean, for one, if we were all to say,
18 great, start today, I mean, I imagine this would follow
19 Longhorn by a few years, so we're not talking about, you
20 know, that whole panel that couldn't sleep at night.
21 They've got a long way to go.

22 I think that you can look at trusted
23 relationships between files and applications inside the
24 PC and start to establish the beginnings of sandboxes.
25 They don't have to go to the ceiling to be effective

1 walls.

2 So I think there is an opportunity there that
3 doesn't have to take place in the OS that can be sooner
4 to market and that can be part of an overarching
5 technological solution.

6 In many ways, I think there's a parallel
7 construct here. We heard a couple of times the cry for
8 overarching privacy legislation that takes us out of the
9 every time we hit a border skirmish we talk about it.
10 Today it's spyware. I suppose we can reconvene here next
11 year to talk about fishing.

12 The same thing happens technologically. The
13 long-term design of the systems and the applications that
14 ride thereon need to be thoughtful in terms of how
15 privacy and security get implemented. And I think things
16 like sandboxes are really interesting, and I think that
17 today we don't have to start at the OS to actually start
18 to implement the concepts.

19 MS. THOMAS: Well, that kind of brings me to
20 the next question about what about a lockbox for the
21 computer's basic configuration file; i.e., the registry?
22 For example, when a program wants to change the registry,
23 an alert would be generated saying Program ABC wants to
24 install itself on your hard drive, or Program ABC wants
25 to change your browser home page. Is that okay with you?

1 Is that a possible idea?

2 MR. MOLL: From a company that just tripled its
3 support staff in the last couple of months, I don't see
4 that -- again, I think you can do these kinds of things
5 from a functional standpoint. I think that the real rub
6 comes into how you interact with the user. And that's a
7 human user. Eight hundred million PCs speaks to who's
8 using them. It's not just a bunch of PhDs in rooms like
9 this. It's everyday folks. It's my three-year-old
10 daughter.

11 And those kinds of warnings unfortunately
12 create I think more often the problem of either being
13 ignored altogether or confusing when listened to, than
14 they solve the problem that we're trying to fix here.

15 MR. FRIEDBERG: I would like to just point one
16 thing out. Unfortunately -- well, the registry is a
17 common place for state for most programs, and there's
18 just all sorts of stuff in there. If you were to get a
19 message every time anything ever changed, you would never
20 get to do your program because you'd be saying yes all
21 the time.

22 And, of course, it's very hard for any
23 individual to make those kind of trust decisions. So,
24 clearly, the challenge would be granularity. What are
25 the most critical elements that need this kind of

1 protection? We've already identified some of them. For
2 example, your desktop user experience, especially around
3 your Internet browsing, you know, home pages should not
4 be hijacked. End of story. It's not something that
5 should be allowed. And if anybody is being able to do
6 it, then we need to find that hole and plug it
7 immediately.

8 And so we have special interfaces for setting
9 the home page which put the user in control. And if
10 anyone's going around those, then we want to know about
11 it and we're going to go after it.

12 MS. THOMAS: Well, would it be possible to just
13 protect the most critical parts of the registry?

14 MR. FRIEDBERG: I think again, you know,
15 theoretically, yes. In fact, that's part of what that
16 exercise is -- look at those key elements, if they happen
17 to live in the registry. Sometimes those key elements
18 may not live in the registry. You still want to protect
19 them.

20 For example, things that automatically run on
21 the system, what's called the run key, and there's a
22 couple of them around. Looking at those kinds of things
23 and trying to decide what meaningful communication we
24 have with the user about what it means when something
25 wants to keep restarting each time you reboot your

1 computer, maybe that's a tipoff of what kind of program
2 this is and what its intent is, in combination with other
3 things.

4 MS. THOMAS: I want to go back to a few other
5 possible tools available at the desktop level. What
6 about if the user has what I'll call a rollback or a
7 reverter, system restore type program? Will that help
8 deal with spyware? You know, you didn't know when you
9 got it. You now know you've got it. It's doing
10 something to your system.

11 MR. FRIEDBERG: I'll actually take this one
12 right now. My mom got that situation with the CD tray
13 opening and closing, and she was asking what's going on.
14 And before I had a chance really to help her, she
15 actually used the rollback functionality on the system.
16 I was really surprised. I don't think most people would
17 do this. But XP has the ability to do system restore
18 points. And every time you install something big, you
19 could roll back to one of those points.

20 Now the problem of course is that you're going
21 back in time and you're also going to get rid of other
22 interesting things you might have loaded, like drivers
23 for a new printer. But at least it gets you back to a
24 stable state. So in some cases I think it could be
25 useful. But I wouldn't call it a general tool.

1 MR. MOLL: Given the number of types of
2 technological solutions we've been talking about that are
3 either proactive or early lines of defense, this seems to
4 me to be a station of last resort.

5 MS. THOMAS: Steve, did you? No?

6 MR. BELLOVIN: What they said.

7 (Laughter.)

8 MS. THOMAS: Okay. And one more question.
9 Then we're going to go to a couple of questions from the
10 audience. We heard a little bit about programs that say
11 they're anti-spyware and they may actually be spyware, or
12 I know that if you do a search for anti-spyware product,
13 you're going to come up with gobs of search results. Is
14 there a need for certification of anti-spyware programs?
15 I.e., that they perform as they claim, such as ICSA Labs
16 does for anti-virus software now?

17 MR. MOLL: I think there absolutely is. I
18 think that this space grew up with a couple of hobbyists
19 really behind it, and rapidly it's evolved into a pretty
20 serious element within an overarching security space for
21 the Internet.

22 The point where today we can find somebody who
23 is capable of coding an application all by themselves,
24 posting to a site and it's rapidly disseminating, I think
25 places us in a position where we can tell cats from dogs,

1 and it's not so easy anymore. In fact, we got a piece of
2 very inflammatory e-mail in our support group about a
3 week ago that it completely confused us with one of the
4 applications that is spyware masquerading as anti-
5 spyware.

6 If there is not some effort -- ICSA is one
7 point. I think COAST is another, and I think some of the
8 guys are here from COAST today. It's the Consortium of
9 Anti-Spyware Technologies, and I think yesterday
10 celebrated its one-year anniversary.

11 So there are some beginnings. I know ICSA is
12 thinking this over. They're not quite ready. But as
13 soon as it can be, there could, one, be some
14 certification of what really isn't anything other than
15 what it's claiming to be; namely, good anti-spyware.
16 But, two, the minute you have that definitional
17 construct, be it for legal purposes and/or for best
18 practices, an organization that can start to use that for
19 a Good Housekeeping seal would also be I think a really
20 good implementation.

21 MS. THOMAS: In other words, if you're going to
22 start looking at the number of, quote, "spyware" that a
23 program found, you need to have agreement on what's
24 spyware?

25 MR. MOLL: You better believe it. I mean

1 that's -- the whole thing kind of hangs together.

2 MR. BELLOVIN: We need definitions very
3 clearly, but I think almost more for enforcement action
4 by the FTC and other law enforcement agencies, a
5 certification, a company, nonprofit or whatever, only
6 works if the consumers know to trust it. Trustee, which
7 is the best know, is not -- my perception, and I'll be
8 happy to be proven wrong -- is that it doesn't have great
9 brand recognition among general consumers. I know what
10 it is. Lots of people in this room know what it is, but
11 I don't think most people do.

12 And you get spyware. The Association of
13 Spyware Peddlers will certify things, too.

14 (Laughter.)

15 MR. BELLOVIN: Although they'll use a slightly
16 different name. But until people know what to look for.

17 MR. WEITZNER: I think it's hard to find in the
18 Internet space many examples of that really working.

19 MR. BELLOVIN: Yeah. That's my concern.

20 MR. WEITZNER: I mean, I think that people come
21 to trust individual pieces of software either because of
22 word of mouth or because of traditional brand-building
23 activities. It's not really obvious to me that there are
24 -- I think there are great sort of self-certification
25 groups like the NAI that have come together to get

1 certain things done, and they certify themselves to each
2 other. But they're really not certifying themselves to
3 the user base that's out there.

4 And I think -- so I think these groups of
5 vendors getting together has a lot of value, but it may
6 not be the kind of value that we associate with the Good
7 Housekeeping seal of approval.

8 MR. BELLOVIN: Right.

9 MR. MOLL: At the end, though, you know, we had
10 Semantic and McAfee, our network associates, both up here
11 on the dias today. I mean, that's like \$20 billion worth
12 of market capitalization right now. They've managed to
13 establish a pretty mature industry with that Good
14 Housekeeping seal. And I think that's, for me, the
15 tightest analog that I can find to spyware is the anti-
16 virus world.

17 MR. BELLOVIN: Well, they've got the brand
18 names, and all the little anti-virus companies, the fact
19 that they claim to be certified by some anti-virus
20 organization doesn't help the consumer. They don't have
21 the brand awareness. It's the brand awareness and the
22 product performance over the years that has helped. And
23 that's what it's going to take.

24 MS. THOMAS: Okay. Here's a quick question
25 from the audience. This is I guess for the anti-spyware

1 vendors. Describe the worst case example of a security
2 breach caused by spyware.

3 MR. WEITZNER: Half Life 2.

4 MS. THOMAS: And what did it cost?

5 MR. WEITZNER: Well, it caused them a launch of
6 a hot game product before Christmas. You know, when
7 somebody's source code gets posted to the Internet, it
8 actually was a Q4 example where a keylogger was deposited
9 on I believe it was the chief architect's machine, and
10 ended up with the game source code on the web. I think
11 that's pretty egregious.

12 MS. THOMAS: Okay. Wayne?

13 MR. PORTER: When we talk about keyloggers, I
14 think it's important to make a distinction. You know,
15 keyloggers can definitely be used for bad, you know,
16 there's a large population out there who use them for
17 monitoring their employees or they use this for
18 monitoring their children. As a matter of fact, they're
19 often sold as child monitors to protect them against
20 pedophiles.

21 One of the most I guess worst security breaches
22 that we saw was a very popular piece of software that was
23 used for child monitoring, which I might add is commonly
24 used by spouses. It's used -- we'll buy it for our
25 child, but it's used to spy -- as a matter of fact, we've

1 actually seen, you know, a couple in the same household
2 spying on each other.

3 (Laughter.)

4 It's usually the first one that wins. But in
5 this case, the software was so poorly coded that they
6 actually -- they used the same password. They hard coded
7 the password. It was made for remote monitoring. So by
8 actually buying the software, they thought they were
9 protecting their children or spying on their wife or
10 husband, they were actually opening up their machine, you
11 know, wide open.

12 MS. THOMAS: Okay. And then the very last
13 question. Spyware has clearly become a large problem
14 today. Where did we as an industry fail, and what could
15 we have done differently?

16 MR. MOLL: I think it's pretty early in the
17 game to call it a failure. You know, I see the presence
18 here is in my eyes a sign of success. We're talking
19 about a problem that two years ago nobody in this room
20 had heard about. We're talking about a problem with an
21 opportunity to solve it from a policymaking and a
22 technological and a best practices and probably a few
23 other levels I'm not thinking about.

24 I'm encouraged by where we are in this thing,
25 and I personally feel that we today have a better jump on

1 this than we had on spam.

2 So I hope that we have a more rapid success in
3 the defense.

4 MR. BELLOVIN: It seems to be my role here to
5 be disagree with people.

6 (Laughter.)

7 MR. MOLL: It usually seems to be me, Steve.

8 MR. BELLOVIN: I think there are a number of
9 mistakes we can point to, but to me the biggest mistake
10 the industry made was deploying mobile code without
11 adequate safeguards.

12 The scariest thing that I heard today was it's
13 possible to write an ActiveX control to scan a machine
14 for spyware. You have a control that's that powerful
15 that can roll with those permissions, my God, what else
16 could it have done?

17 MR. WEITZNER: And I would just, sort of to
18 piggyback on that. I think the mistake, if you could
19 call it one, was to hook up hundreds of millions of PCs
20 with operating systems that weren't really designed to
21 work on the Internet. And there's been a huge amount of
22 effort to catch up on that, and I think to everyone's
23 credit who's been involved.

24 But it was not really expecting that there was
25 going to be this thing called the Internet or the World

1 Wide Web that was going to be this extraordinarily
2 powerful distribution medium for both content but also
3 for malicious code.

4 And I don't think that's really a mistake, but
5 I think that is the fact of the matter of where all this
6 stuff comes from. It comes from the web. It comes from
7 the Internet. And I think everyone's working hard to
8 catch up to that.

9 MR. BELLOVIN: We'd have to go back to making
10 an honest living, Danny boy.

11 (Laughter.)

12 MS. THOMAS: And I'm not surprised Jeffrey
13 would like to speak, too.

14 MR. FRIEDBERG: I do want to point out, and I'm
15 sure Steve can back me up on this, you know, the Internet
16 and the Ethernet and the Arpanet, I mean, this stuff has
17 been around for a long time. And there was originally a
18 code of ethics with respect to use of the technology.

19 He's shaking his head. He knows this. And,
20 you know, as things kind of progressed, eventually
21 suddenly it became not just for the scientists but for
22 the rest of the world. And as the doors opened up, so
23 did economic incentives. And we're seeing a huge amount
24 of that as drivers towards bad behavior.

25 And we've yet to have any of the right, you

1 know, processes in place to kind of keep that in check,
2 and that's what this is all about I think. It's just a
3 natural progression of what's been happening.

4 So actually, I really look forward to what's
5 been going on here today, look forward to working with
6 other industry partners on best practices and everybody
7 else that can possibly contribute, because it's going to
8 make my life a lot better when I use my system and my
9 family's going to use their system. So, I think this is
10 definitely on the right track.

11 MS. THOMAS: Okay. So to sum up, there are
12 tools at the desktop that individuals can obtain to help
13 reduce but not eliminate unwanted spyware, and it sounds
14 like there are some technological measures that could be
15 developed at the network, browser, and operating system
16 levels.

17 However, as people have been saying throughout
18 the day, some of these depend on establishing better
19 definitions of spyware or some best practices.

20 SO it sounds like no one is there yet, but more
21 and more companies are working on it.

22 So I'd like to thank you guys, and please
23 everyone stay seated, because we're going to go straight
24 to the next panel. So, thank you.

25 (Applause.)

1 (A brief recess was taken.)

2 MR. PAUL: Everyone please take their seats,
3 please.

4 Thank you, everyone. We're just about ready to
5 start our last panel of the day, which is going to be
6 Government Responses to Spyware.

7 I'd like to introduce the moderator for our
8 last panel. Our moderator is Beth Delaney. And, Beth,
9 if you'd like to begin with the last panel, that would be
10 great. Thank you.

11 MS. DELANEY: Okay. I'd like to thank everyone
12 for staying until the very end. And also, once again,
13 I'd like to thank our coffee sponsors for keeping us
14 awake and alert all day, and that's the Online Privacy
15 Alliance and the law firm of Hogan & Hartson.

16 For our final panel we have a very interesting
17 group of people here, and I'm sure you're going to find
18 them worth the wait.

19 We've heard a great deal of information today
20 from a variety of different panelists, and after lunch
21 we've been focusing on the responses to Spyware. The
22 first panel after lunch looked at industry responses, and
23 the second panel focused on technological responses.

24 This panel is going to discuss how the
25 government can play a role in responding to concerns

1 about Spyware, including law enforcement, legislation,
2 business outreach, and consumer education.

3 Time permitting, we'll also take questions from
4 the audience and we'll again use the same procedure,
5 where Shakeel is walking around, collecting the question
6 cards. So if you have a question, write it down on a
7 card, and he'll pick it up from you.

8 I'd like to start out by briefly introducing
9 each of our panelists. On my left is Jennifer Baird.
10 Jennifer is legislative counsel for Congresswoman May
11 Bono of California.

12 In July 2003 Congressman Bono introduced the
13 Safeguards Against Privacy Invasions Act, also known as
14 the Spy Act.

15 To Jennifer's left is Mark Eckenwiler, Deputy
16 Chief of the Department of Justice's Computer Crime and
17 Intellectual Property Section. Mark's areas of
18 responsibility at DOJ include federal wiretap law,
19 computer search and seizure, and online investigations.

20 To Mark's left is Mary Engle, an associate
21 director of the Bureau of Consumer Protection here at the
22 FTC. Mary leads the Bureau's Division of Advertising
23 Practices, which is the division that's actually running
24 this workshop today.

25 The division is responsible for regulating

1 national advertising matters, including claims about
2 food, over-the-counter drugs, dietary supplements,
3 alcohol, tobacco, and online advertising.

4 To Mary's left is Elizabeth Prostic, who is a
5 Managing Director with the Public Law and Policy
6 Strategies and Information Security and Internet
7 Enforcement Groups at the law firm of Sonnenshein, Nath &
8 Rosenthal.

9 Until just last week Elizabeth was at the
10 Department of Commerce, where she served as Senior Policy
11 Adviser to Secretary Donald Evans and also as chief
12 privacy officer.

13 To Elizabeth's left is Matt Sarrel, who's the
14 Technical Director at PC Magazine. Matt leads the
15 testing teams at PC Magazine, and he'll talk to us about
16 the consumer education efforts that they've engaged in.

17 And last, but certainly not least, is
18 Representative Stephen Urquhart from the Utah House of
19 Representatives. Representative Urquhart sponsored the
20 Spyware Control Act, which is the first Spyware
21 legislation that was signed into effect, and that was in
22 Utah.

23 And also if I could just remind the panelists,
24 feel free to speak directly into the microphone. They're
25 very small and you need to get up really close to them.

1 Let's start by finding out about current law
2 enforcement efforts. Mary, during today's testimony
3 we've heard about some of the concerns related to
4 Spyware. What is the FTC planning to do to respond to
5 these issues?

6 MS. ENGLE: Well, I think the first thing we're
7 going to do is digest everything that we've heard today,
8 and, hopefully, we won't get indigestion as a result of
9 that. I think, actually, it's been a very good
10 discussion and a lot of really helpful comments.

11 In addition, there's quite a written record,
12 people have submitted written comments. And we'll
13 continue and we'll look at those as well.

14 And then we'll have a report that we'll issue
15 following up on this. And as people have mentioned, over
16 the years, the Commission has held workshops on a number
17 of these emerging technology issues, and one of the
18 things that we hope to do is, where we see some heat
19 going on, shed a little light on the issues. And that's
20 one of the functions that we have here at the Commission,
21 in addition to our role as a law enforcement agency. And
22 we do have a couple of investigations underway right now
23 regarding Spyware, and we would expect that those will
24 see the light of day before too long.

25 We also have our consumer and business

1 education role to play, and as has been discussed
2 throughout the day, there's a real need for consumer
3 education in this area, both for parents and their kids.
4 I mean, kids probably don't care too much about the harms
5 that may cause, so the parents really need to know what's
6 going on and what steps they can take.

7 And, finally, I think, as Commissioner Thompson
8 had suggested, we're really interested in self-regulation
9 in this area and best practices and working with industry
10 to see what we can do to encourage those.

11 Could you just sketch out for us, what would
12 you look for in a Spyware case, just to get everyone on
13 the same page in terms of the different components.

14 MS. DELANEY: Well, to bring a case, the
15 Federal Trade Commission would have to prove that a
16 particular action was unfair or deceptive under the
17 Federal Trade Commission Act. And I won't try to define
18 those terms here, but they do have particular legal
19 meanings, and the bottom line for both of it is that
20 there's some consumer injury, that some harm has occurred
21 to consumers.

22 And I think that that was -- I was interested
23 to hear the discussion this morning in the first panel
24 about defining Spyware, and there was some concern that,
25 you know, you really couldn't come up with a definition

1 without inadvertently including positive software.

2 But for us, you know, it doesn't matter what
3 it's called. What matters is what happens -- what
4 happened as a result, what's the harm that's caused to
5 consumers. And if there is harm, whether it's slowing
6 down the consumer's PC or causing it to crash or causing
7 them to have to reset their browser repeatedly or what
8 have you, there are lots of different types of harm that
9 we would find actionable under the Federal Trade
10 Commission Act.

11 And so we could look at those, and then
12 assuming we were able to identify the perpetrator --
13 which is an issue, and it's been alluded to earlier. A
14 lot of times, you know, people hide themselves pretty
15 well, and it takes a lot of investigation to actually
16 find who is behind this, as is true in the spam arena as
17 well, or it may be located overseas, and so that's a
18 difficulty as well.

19 But I think the main thing is to -- if the
20 practice is causing harm to consumers -- and I would say
21 harm that's sort of quantifiable in some way, more than
22 just sort of, well, I don't like the idea that someone
23 may be tracking be around, and nothing really comes of
24 it. Then we could bring a case there.

25 Mark, we'd like to hear about the Department of

1 Justice's perspective on the issues associated with
2 Spyware. Can you first tell us a little bit about the
3 current statutory authority that you work with?

4 MR. ECKENWILER: Sure. In many ways that goes
5 back to the discussions the various panels have been
6 having since the very beginning of the workshop this
7 morning about the different kinds of behaviors that we're
8 talking about when we use this umbrella term, Spyware.

9 From my perspective, one of the major
10 dichotomies would be looking at subversion of a machine,
11 taking over control, in part or in its entirety, of a
12 particular machine, or maybe altering some setting and
13 making it difficult to alter the setting.

14 That really doesn't implicate a privacy
15 concern. You know, if I changed your home page, I really
16 haven't impaired your personal information. I haven't
17 disclosed something that you sought to keep confidential
18 to someone else.

19 On the other hand, you may have privacy
20 invasions. And to give you a sense of what the statutes
21 are that would cover each of those halves, there's
22 something called the Computer Fraud and Abuse Act,
23 originally enacted in 1984. It's gone through a series
24 of iterative amendments, probably about every four to six
25 years.

1 One of the main prongs of that, Section 1030-
2 A(5), speaks to impairing the integrity of -- basically
3 it says causing damage to a protected computer, without
4 or in excess of authorization. And as we'll discuss a
5 little bit later, that's one of the rubs in this area.

6 So we certainly have a statutory tool for
7 dealing with those kinds of subversion attacks from
8 Spyware. In fact, that's the same statute that I would
9 use to prosecute a denial of service attack or your
10 typical network intrusion.

11 On the other side, the privacy side, there is
12 an array of statutes that we have, depending upon the
13 particular behavior. There's another section of Section
14 1030 that goes to the acquisition of data from a
15 protected computer without or in excess of authorization.
16 That, again, has a fairly arcane series of different
17 elements, aggravating factors, maybe a misdemeanor, maybe
18 a felony, depending on the circumstances.

19 Spyware, if it's, say, a keylogger, could in
20 fact impact the wiretap statute, Title 3, and there's a
21 companion statute that deals with the manufacture or
22 trafficking, advertising of the availability of we call
23 them interception devices. Our position would be that
24 includes software.

25 And then, last of all -- this I don't think

1 even exhausts the list of current statutes -- there's
2 also a statute, Section 1029, right before the Computer
3 Fraud & Abuse Act, that deals with so-called access
4 devices, originally intended to deal with things like
5 stolen credit cards, but can also be made applicable to
6 stolen passports.

7 So, for instance, if you have a keylogger, the
8 keylogger may implicate not only the wiretap statute, but
9 if there is acquisition of a bunch of passwords from the
10 user acquired with fraudulent intent, they may also run
11 afoul of one of the various subparts of Section 1029.

12 MS. DELANEY: Okay. Has the absence of
13 specific Spyware legislation been an impediment to your
14 law enforcement efforts?

15 MR. ECKENWILER: I think, by and large, the
16 answer is no. As I think my previous answer may have
17 communicated, we have in our quiver a number of arrows
18 that we can use in prosecution. Let me just give you a
19 couple actual examples.

20 One of the members of the previous panel
21 mentioned the Kinkos case, a defendant named Juju Jon up
22 in New York City who installed Spyware on a number of
23 terminals in a Kinkos. He pled guilty last year to a
24 five-count information, three felonies, two misdemeanors,
25 under a variety of -- basically many of the statutes that

1 I just named, Computer Fraud & Abuse Act, the access
2 device statute.

3 He hasn't been sentenced yet. He's going to be
4 sentenced on May 10th. But certainly we did not
5 experience a bar in that case.

6 Looking forward, just last month the U.S.
7 Attorney's Office in Los Angeles unsealed an indictment
8 against a gentleman named Larry Lee Ropp, accusing him of
9 installing a keylogger on a machine at his former place
10 of employment. And so he's now been charged with
11 endeavoring to intercept communications in violations of
12 the wiretape statute.

13 MS. DELANEY: Right. Is that the one that used
14 the Whistleblower Act as a defense?

15 MR. ECKENWILER: I don't want to comment on it.

16 MS. DELANEY: That's fine.

17 MR. ECKENWILER: But, I mean, there's no
18 defense yet. This case, you know, if it ever goes to
19 trial, we'll find out what his defenses are. But,
20 certainly, as I understand it, there have been some
21 public statements about how this could -- he apparently
22 believes it could be justified as some sort of
23 whistleblower action. That's certainly not our view.

24 MS. DELANEY: Mary, I'd just like to quickly
25 ask you the same question. Has the absence of specific

1 legislation been an impediment?

2 MS. ENGLE: No, not to this point. As I
3 indicated, if there's harmful conduct, that's what we're
4 going to -- or conduct that results in a harm to
5 consumers, that's what is going to drive us, and we have
6 adequate remedies to deal with that right now. We're not
7 so much driven by a particular definition.

8 MS. DELANEY: Okay. What I'd like to do now is
9 just to kind of move into the different legislative
10 efforts that people are working on.

11 Jennifer, in a nutshell, what are the basic
12 requirements set forth by the Safeguards Against Privacy
13 Invasions Act?

14 MS. BAIRD: I'll try to put it in a nutshell.
15 As you know, the congresswoman introduced HR 2929 in
16 July, and we have been working on what Mary referred to
17 and what CDT referred to earlier in the first panel
18 regarding the difficult issues as to how to define
19 Spyware and et cetera, et cetera.

20 What my boss found when she learned about
21 Spyware is that a lot of times when people download
22 Spyware currently, if you were to try to prosecute them
23 or bring a law enforcement action against them, you
24 wouldn't necessarily have any tools available just
25 because they are giving notice.

1 However, it is not -- and they could easily argue that
2 it's clear and conspicuous.

3 However, very few consumers actually read the
4 notices or know what they say. So even though there is
5 notice and there's -- you know, it's kind of check that
6 box, that's been done, it's not effective, and people
7 don't know what they have on their computers, and they
8 don't know what it's doing or why their computers are
9 running so slowly.

10 So what my boss's bill would do is basically
11 require a notice regime that really puts it in the
12 consumer's face as to what they're downloading and really
13 asks them to decide whether or not they want to continue
14 with the downloading process.

15 And that is done in a couple different ways.
16 The first component would be a -- of course, something
17 being included in the license agreement. The second one
18 would be when someone is downloading Spyware onto their
19 computer, there would actually be a downloading notice.

20 And what that means is, at each affirmative
21 step that the computer user took to download Spyware, it
22 would explain this is what this program is, it's Spyware,
23 this is what it does, this is the information that we may
24 collect, this is what we may do with it. If we do
25 collect it, do you want to continue?

1 So it just makes it much clearer for the
2 consumer and -- in other words, if a consumer were to
3 consent to Spyware, technically they should never be
4 spied on, even though it is Spyware, because they will
5 have chosen what they want to download onto their
6 computer and what information they want to share with
7 another source.

8 MS. DELANEY: Earlier in the day it was
9 suggested that some of the proposed legislation defining
10 Spyware is too broad. Can you comment a little bit on
11 that?

12 MS. BAIRD: Sure. This is -- as I said, this
13 is a difficult issue as far as -- we all know that
14 keylogging, for example, has very potential devastating
15 effects, and that Spyware, of course, could be a
16 magnificent tool for identity theft and et cetera, et
17 cetera.

18 However, it's difficult to define Spyware to
19 where it targets the behavior that you want to target
20 without targeting more, without -- for example, there are
21 -- and my boss's bill does not cover this, and neither
22 does the Senate bill, but there are some programs that
23 you could argue have Spyware capabilities that are great
24 programs.

25 Antivirus software, for example, it has that

1 sort of capability to where it can see what's on your
2 computer and what's going on so that it can prevent, you
3 know, infection through viruses on your computer.

4 There are some programs that provide technical
5 support that have some sort of Spyware capability.

6 And then there are the sort of things that
7 people are saying this should not cover, and we, by no
8 means -- my boss, by no means, wants her bill to cover
9 that, and we have been working hard to make sure it
10 doesn't.

11 I've heard a lot of different things today.
12 I've been here since about 9:30, so -- and I appreciate
13 that you all stayed. I was expecting the room to be
14 empty by the time we sat up here.

15 But some of them were -- the first thing that
16 the first panel mentioned, well, you have to look beyond
17 the notice and consent, and you have to look beyond the
18 requirement that it be easily installed, which my boss's
19 bill does require, and you have to look at what's in the
20 middle.

21 And also the argument that we need broader
22 privacy legislation, we need a big privacy bill.

23 Another thing has been -- another thing that we
24 heard from industry has been, you know, self-regulation
25 is the answer, but we can't really come up with best

1 practices yet.

2 So, in other words, what we're hearing is, this
3 is a problem, it needs to be solved, but we don't know
4 how, so just hold on.

5 And that's not how it works in Congress, and,
6 you know, as a member of Congress, my boss has the
7 responsibility to do all she can to protect her
8 constituents from downloading onto their computer that
9 they use for personal, you know, banking and for credit -
10 - you know, buying things through their credit card and
11 so on and so on. She has the responsibility to make sure
12 that they have confidence when they're using their
13 computer, and that that information won't be shared.

14 And another thing that, of course, has been
15 said is, legislation is just the wrong answer. This can
16 only be done through self-regulation.

17 I would say that we can't sit around and just
18 think about it and talk about it for days and nights in a
19 year, we do have to act. But that being said, I do think
20 that industry self-regulation is a very important aspect
21 of this, and my boss understands that legislation by
22 itself will not stop the problem, but it is a step in the
23 right direction. It is a step in the right direction
24 that people know what they're downloading onto their
25 computer before they download it.

1 It's a very basic concept, and they should
2 know. They should not be downloading something onto
3 their computer that they are not aware of.

4 And so I guess the general message that I'm
5 trying to get across is, something has to be done. It
6 might not completely solve the problem, but there are
7 some very basic things that we can do to make sure that
8 Spyware is at least slowed down a little bit.

9 MS. DELANEY: I'm just going to ask you one
10 more quick question. And if you could just tell us the
11 major differences between your bill and the Senate's
12 Spyblock Act.

13 MS. BAIRD: Okay. The Senate bill covers
14 software in general, and when I say software in general,
15 what I mean is the notice and consent regime does not
16 only apply to Spyware. It applies to all software.

17 It also has a red herring notice which is --
18 implied in my boss's bill is that it's not set apart,
19 which basically says that it is wrong to deceive or
20 mislead someone into downloading something that they do
21 not know that they're downloading.

22 Another thing is that my boss's bill only for
23 enforcement gives the FTC the ability to enforce the
24 bill. The Senate bill gives state attorneys general the
25 ability enforce the law as well.

1 MS. DELANEY: Okay, thank you very much.

2 Let's move to the state perspective on Spyware
3 legislation. Representative Urquhart, your state passed
4 the first piece of legislation specifically directed to
5 Spyware.

6 Could you first tell us a little bit about the
7 problems that your law was designed to address?

8 MR. URQUHART: Sure. It was designed to
9 address the problems that we talked about here today.
10 First -- well, first, let me tell you some things that it
11 doesn't do. There's a lot of myths circulating around
12 the bill.

13 First is, it does not ban porn filters. Check
14 that out on Section 1027. It does not ban instant
15 messaging. That's clear in 102(b)(2).

16 So what it does so, it first addresses
17 disclosure. If we can put up on the screen -- someone's
18 helping me out. Here's a standard Adware disclosure.
19 Okay, now, you look at the terms there on the bottom
20 left, we have seven lines of text with about two or three
21 -- you can go to the next one -- two or three words per
22 line. Okay, thank you, that's fine.

23 So there that's not inviting consumers to learn
24 about the product. That's defying them to read legalese
25 through a straw.

1 You compare that to the Google tool bar here,
2 you have many lines of text appearing on a screen. Now,
3 this first one, this is to protect Google and their
4 property. So you can go to the bottom there and just
5 hit, okay, I agree with that.

6 Go to the next one, please.

7 Now, this is one protecting consumers. Look up
8 at the top there in the red. They're pointing out this
9 is not the usual yada yada. They're begging people to
10 read their disclosure policy. Then down there at the
11 bottom you have to click on a feature. So you're forced
12 to actually pay attention and do some reading.

13 Now, there's a world of difference between
14 those two.

15 So in this area what we did, and what we would
16 encourage policymakers to do would be to study consumer
17 knowledge and perceptions, and we've heard today that 75
18 percent of the people with Adware don't know they have
19 it, they don't know how they got it. So we can't call
20 those people consumers; they're victims.

21 So I would say a law legitimizing current
22 practices would be a significant step backward. So we,
23 first off, beefed up disclosure. Secondly, we addressed
24 removal. We've had a lot of discussion on that today, so
25 I won't discuss that.

1 I'll go to my third and last point, which is --
2 we deal with context-triggered popovers, and these are
3 ads triggered based on the content of a web site without
4 any affiliation to that web site.

5 And so the policy question here is, is this
6 good old-fashioned American competition or is it
7 parasitic? And we concluded unanimously that it is
8 parasitic, and the host of that parasite is commerce.

9 And we concluded that Adware threatens commerce
10 in two ways. First, it hobbles the Internet. When users
11 are burdened, frustrated, even frightened by undisclosed
12 invaders, then they're going to avoid that technology.
13 They're going to shy away from e-commerce.

14 And, secondly, we think that Adware destroys --
15 and I'm talking Adware under current practices, like the
16 first disclosures you saw. It destroys investment-backed
17 expectations. So, again, policymakers here had to weigh
18 the burdens and benefits to commerce.

19 Now, I'd encourage you to think of a lemonade
20 stand. Commerce values the legitimate competition of
21 several more lemonade stands. That's good. Commerce
22 does not value the illegitimate competition of stealing
23 lemons out of the orchard. In the marketplace of e-
24 commerce, the lemon grove is planted and tended by web
25 site owners and affiliated marketers, and currently

1 they're being harmed.

2 You've got to remember that in the short term,
3 the best deal for consumers is shoplifting. Nothing
4 beats the five-finger discount. But in the long term, if
5 investment-backed expectations are trampled, then the
6 marketplace and consumers will suffer.

7 And vendors need a little space in the
8 marketplace. That's why the butcher, the baker, the
9 candlestick maker, they have little expectation for
10 privacy out in the public, but in their shop, no one can
11 camp out at the cash register. And if they're allowed to
12 do this, then the market will shift solely toward the
13 harvest. In other words, the market will shift solely
14 toward stealing purchases at the point of purchase, and
15 it will move away from planting and tending the orchard,
16 and that would be developing and branding a web presence.

17 So those are the things that we addressed. I
18 really enjoyed hearing Jennifer's comments. I agree with
19 them 100 percent. I think that unless there is
20 regulation in this area, the butcher, the baker, the
21 candlestick maker, they'll stick to brick-and-mortar if
22 their sales can be stolen at the point of purchase in one
23 context, and not the other, and then consumers also will
24 shy away from this wonderful technology.

25 MS. DELANEY: Could Utah's state tort law,

1 something like interference with a prospective business
2 or customer relationship, have been able to deal with
3 some of these issues rather than additional legislation?

4 MR. URQUHART: Arguably they might have. Or
5 especially if you have a statute like California's Unfair
6 Business Practices Act, that might be able to.

7 But I think that that is a horrible way to make
8 law, because those are very blunt instruments. I mean,
9 it's just something unfair that you don't like, and it
10 wasn't created with the Internet in mind. And as a
11 result, it would be left up entirely to the courts to
12 flesh out policy and flesh out law in this arena, and a
13 better way to do it is to have legislatures specifically
14 look at all the things and use a nuanced approach, which
15 is what we did, and at the end of the day, it bans bad
16 behavior and leaves the good actors alone.

17 I mean, we've heard a lot today about Adware,
18 how it really bogs down people's computers. It's really
19 a problem. Well, we've had one Adware company say that
20 my bill, even though it hasn't gone into effect yet, has
21 cost them tens of thousands of downloads. There are a
22 lot of happy consumers out there by that fact.

23 Another Adware company that is about to go
24 public, they have in their S-1 statement that because of
25 this law, they're going to avoid Utah. That's great.

1 I mean, constituents, they demand results.
2 They're sick of this stuff. And so I've heard a lot of
3 handwringing here today, and I think it is great that we
4 do need best practices, we need education, we need
5 technology, but we also need regulation.

6 I mean, how do you stop bad guys? You have a
7 neighborhood watch? You have education to pick up your
8 newspapers. Don't leave them sitting around. You have
9 technology, you have alarms and bars, but at the end of
10 the day, you've got to have laws and a cop on the beat.
11 And so we've put a cop on the beat.

12 MS. DELANEY: So just to recap, the major
13 requirements for your bill -- or your law is notice and
14 consent, a removal aspect, and then the context-triggered
15 pop-ups?

16 MR. URQUHART: Right. So the bulk of industry,
17 they're fine, because if they do monitor data, if they
18 mine data, then they can provide some consent on that and
19 easy removability.

20 Now, if they do context-based advertising, then
21 there are some significant additional requirements for
22 notice. Tell them what kind of pop-ups they're going to
23 get, how often they're going to get them, and we don't
24 allow them to pop over at the point of purchase.

25 MS. DELANEY: Are there any points you've like

1 to make in comparing your legislation to the different
2 federal legislative efforts?

3 MR. URQUHART: Well, I'm excited about
4 Representative Bono's bill. I think that that's a
5 wonderful start. We need to empower consumers. They
6 need to know what they're getting into.

7 I mean, right now we have an arms race. You've
8 heard that Whenu has been removed 80 million times. The
9 business model there, it's just to dump it on computers
10 faster than people can become educated and get it off.

11 And so that's a very important component.

12 But I think we fall short if we don't deal with
13 the context-based advertising. I think this is very
14 detrimental to e-commerce. E-commerce, just like we do
15 in the real world, you have to defend and back up
16 investment-backed expectations.

17 And so that's an aspect that I would hope the
18 federal -- you know, at some point the federal
19 government's going to preempt this, and I don't pretend
20 that that's not going to happen. But I hope they do it
21 with a beefy, good bill that protects consumers and
22 commerce.

23 MS. DELANEY: Before we move on to outreach to
24 the business community, do any of the other panelists
25 have any comments on what we've covered so far? Okay.

1 Elizabeth, can you tell us about the Department
2 of Commerce's efforts to work with the business community
3 in responding to the concerns and issues raised by
4 Spyware?

5 MS. PROSTIC: Sure. Let me first say that I
6 promised Secretary Evans that I would be on my best
7 behavior since I left the Department four days ago.

8 One of the things that the Department has done
9 under Secretary Evans' leadership, as with past
10 secretaries, is be the advocate for the private sector,
11 promote economic growth -- particularly here we're
12 talking about e-commerce -- and, third, support
13 international trade.

14 And I think that Spyware plays a role in all of
15 those. As we learned in the spam context, you can't just
16 regulate it here, you have to talk about what happens
17 abroad.

18 But what we've done predominantly is open our
19 doors to the private sector and the privacy advocates and
20 to really focus on the larger policy questions, which are
21 balancing the need to protect the privacy of individuals
22 and businesses, while preserving innovation and some of
23 the legitimate practices that the private sector is
24 endeavoring.

25 And this is similar to the approach we've taken

1 on other types of -- in other technologies. With spam,
2 as many of you were here for that evolution, we looked at
3 specific solutions to privacy, self-regulatory
4 approaches, technology solutions, and then, in the end,
5 congress decided, with administration support, that there
6 was legislation needed to track down some of the bad
7 actors, giving the FTC and the Department of Justice
8 authority to enforce certain penalties.

9 So, really, what we've done is to try to open
10 our doors, try to listen to the private sector and to the
11 privacy advocates, and to ensure that we are taking into
12 account some of the larger principles that are specific
13 to Spyware that are not unlike other technology issues
14 that we faced in the past.

15 MS. DELANEY: Have there been specific harms
16 that have been visited upon businesses? Have you heard
17 much from the business community in that regard?

18 MS. PROSTIC: Well, absent legislation, I think
19 that many legitimate businesses are focusing on what
20 current practices could be curtailed, or could be
21 prevented if legislation is enacted, but it doesn't take
22 into account certain definitions or certain practices.
23 So I think it would be hard to pinpoint a specific
24 practice.

25 But, really, right now we're focusing on trying

1 to differentiate between practices and activities that
2 are good for consumers and those that harm consumers, and
3 that there's a need to legislatively punish certain
4 violators, in addition to the existing statutes that the
5 FTC and the Justice Department have at their discretion.

6 MS. DELANEY: What I'd like to do now is turn
7 to Matt Sarrel. Matt, as I mentioned before, is the
8 technical director at PC Magazine.

9 First, can you tell us a little bit about why
10 PC Magazine focused that much attention on this issue?

11 MR. SARREL: Well, we -- we took our first in-
12 depth look at Spyware in April of 2003 in an article
13 entitled "Spyware, it's Lurking on Your Machine." So,
14 that was a year before this article that you're
15 mentioning now. And that article focused on describing
16 the risks and prevalence of Spyware -- really defining
17 the problem. Defining what Spyware is, key loggers,
18 Adware, ad cookies -- things like that. And then we went
19 on to review several anti Spyware solutions.

20 Prior to that, we had been looking at the
21 overall issue of Spyware, particularly key loggers, as a
22 lot of them are considered to be viruses for many years.
23 And overall, our readers look to us for guidance in
24 understanding how to deal with the serious nature of the
25 Spyware problem. Our readers really want to understand

1 the effects of Spyware. They want to detect and remove
2 Spyware from their systems.

3 So, at the beginning of this year, we spoke
4 with a lot of analysts who were reporting an explosive
5 growth in both the types of Spyware, and the number of
6 computers infected with Spyware. So we decided the issue
7 was worthy of a large cover story.

8 So then, in March -- well actually, I guess, in
9 January, because it takes us a long time to actually get
10 into print -- we started working on the story that you
11 had there, called Spy Stoppers. It was within a larger
12 package that also contained information regarding
13 identify theft and safe computing. This time, we
14 changed our focus a little, and we felt that we had
15 described the problem fairly thoroughly, and what we did
16 instead was focus on reviewing 14 anti-Spyware tools, and
17 we included several side bars about how to recognize the
18 symptoms of Spyware, and also how to avoid becoming
19 infected in the first place.

20 We feel that the magnitude of Spyware and the
21 issue of Spyware increases as more and more people
22 integrate Internet usage into their daily lives, and that
23 consumers or victims have a right to understand the
24 issue, and what they can do to protect themselves.

25 MS. DELANEY: Right. We've heard a lot about

1 consumer education today, and what I'd like to ask you
2 next is -- you know, from your unique perspective, what
3 can you tell us about what government agencies and
4 consumer advocacy groups need to keep in mind when
5 designing effective consumer education initiatives?

6 MR. SARREL: Okay. Well, first, I want to say
7 that I think everyone here -- what I've heard today has
8 been good in terms of, you know, best practices on the
9 part of the industry, legislative controls, but in my
10 mind -- and it -- you know, of course, it's because of
11 the way that I approach the problem as being involved in
12 consumer education. So, what I think first has to happen
13 is that consumers need to get sick and tired of having
14 this garbage put on their machines. And when consumers
15 can't stand it anymore, that's when something's going to
16 get done, because they're not going to buy the things,
17 they're not going to download the things that come with
18 Spyware.

19 So, along with that comes with -- that I think,
20 in the beginning, what we need to do is educate consumers
21 about what is at stake, and why people should care. So,
22 after we did these two stories, I got so many e-mails
23 from people saying that they didn't care. Who cares?
24 Fine, so there's Spyware on my machine. But, you know,
25 I'm able to download music for free. You know, that I'm

1 willing to make that trade. And I just -- that -- that
2 kind of shocked me, and I even had a discussion with one
3 person who said that she didn't care if a certain item of
4 software was Spyware -- she finds it to be a convenient
5 took for completing web forms.

6 So, I asked her if she would buy a stolen Rolex
7 on a street in Manhattan, hand the guy a business card,
8 ask him to put her name and address in a data base, and
9 then periodically send him updates on her jewelry
10 purchasing habits. So, I think she got it after that.
11 Consumers need real-world examples of these risks to
12 their personal information. A lot of them feel that
13 there's anonymity in numbers, and that they're safe,
14 because it's over the Internet.

15 So, you know, why doesn't everyone just e-mail
16 me their credit card and PIN. People seem to understand
17 that. Right, there's been credit card fraud, people have
18 adjusted their level of understanding to understand, or
19 include, credit card fraud. I think part of their
20 problem is, they just don't get Spyware, and, you know,
21 what it -- what it can do to them.

22 Someone earlier drew the analogy between
23 Spyware and computer viruses, and I think that that's
24 appropriate. And I think back to when I was a network
25 administrator in the early 1990s, and I saw my first

1 outbreak of some boot sector virus that's, you know,
2 probably long gone. I tried to educate my users how not
3 to get viruses, how not to bring them into the work
4 place, things like that, and no one got it. Okay? But
5 now, 15 years later -- well, we'd like to think
6 everyone's running anti-virus software, and that people
7 get it. And hopefully, it won't take 15 years to
8 understand what's wrong with Spyware.

9 So, I think also, in computing, consumer
10 education usually starts with the media. People read an
11 article about something, they become interested about it.
12 Also, people tend to learn things when they go to buy
13 something. And also, people learn from their corporate
14 IT departments. So, you know, PC Magazine and PCMag.com
15 provide a lot of educational material, as do anti-Spyware
16 and anti-virus vendor web sites, and various government
17 sites. There are also specialized web sites that focus
18 on security and privacy issues, including the latest
19 Spyware information, education, and detection and removal
20 tools.

21 Corporate IT departments should train employees
22 -- just like they did with anti-virus software -- they
23 should train employees, and distribute tools to detect
24 and eradicate Spyware, especially on mobile systems, in
25 addition to teaching people how to use software

1 firewalls. And finally, retailers should have virus,
2 Spyware, Malware information centers, or kiosks,
3 subsidized by software vendors.

4 And then the final note I'd like to leave
5 everyone with is that my -- my gut feeling that all the
6 education in the world won't do anything until consumers
7 understand the real risks to personal information
8 inherent to Spyware.

9 MS. DELANEY: You know, that's a great point,
10 because I think we had a phone conversation a couple of
11 weeks ago, and as horrible as some of these virus
12 outbreaks have been, you thought that actually, some of
13 them were kind of helpful in the sense that they -- they
14 made consumers more aware of what was going on, and that
15 actually forced them to buy some of these products, and -
16 - or download them for free, just to deal with the
17 problem.

18 MR. SARREL: Right. That's what -- you know, I
19 get a lot of -- it's funny, I gain a lot of understanding
20 from talking to my friends, or my parents' friends, about
21 the problems they have with their computers, right? So,
22 what do they have? They have pop-ups. They have -- the
23 machine's running slowly, they don't understand why. You
24 know, maybe they have -- they have got a worm that's
25 using up all their band width. But they don't understand

1 that. What -- what they understand is, they -- they
2 can't do what they want to do.

3 And for now, my comment about the viruses,
4 because a lot of these worms don't really carry a lethal
5 payload. So, they're -- they're sort of just people
6 trying to get attention. And, you know, when they get
7 attention, they disrupt the way that you use your
8 machine. And what I'm -- what particular concerns us is
9 that somewhere in between all of these things spreading
10 so easily and so quickly, is going to come something that
11 has a big payload. Or, the Spyware that, you know,
12 really takes everything away from you. And I think
13 people need to understand what the risks are, and just
14 get -- be sick of the risks, and take the precautions
15 that they need before anything really happens.

16 MS. DELANEY: We have some questions from the
17 audience, so I'll give -- Does any other panelist want to
18 add anything at this point, before I move into that? We
19 have -- the first question is for Mark. "You mentioned a
20 few cases where use of a key logger was prosecuted. Have
21 there been cases where authors have been investigated or
22 charged, and is there a legal framework to use for
23 authors under current law?" So it would be the -- the
24 people that were writing the key loggers.

25 MR. ECKENWILER: You could, in theory, bring a

1 prosecution under Section 2512. Certainly, it's a more
2 attractive case from a prosecutive standpoint, if you
3 have the person actually trafficking in it, and actually
4 making this available as a commercial product for sale,
5 actually deployed out in the market place. So yes, I
6 think, you know, in -- in most cases, we would have a --
7 a mechanism for going after someone at least who's
8 trafficking. I'm -- I'm not sure that 2512 would apply
9 strictly to someone who just created such a product.

10 And of course, the -- the thing to remember is,
11 there are other -- there are interception tools all over
12 the place, many of which are used by system
13 administrators, just to do network diagnostics, so there
14 -- there is certainly a -- I'd say it's a fine line, but
15 in fact, it's a very fuzzy line, there, about what's --
16 what's appropriate and what's inappropriate in terms of
17 monitoring software.

18 MS. DELANEY: We have a question for Jennifer.
19 "Since Justice and the FTC both said that no new law is
20 needed to prosecute where consumer harm can be shown,
21 what is the need for your bill, specifically?"

22 MS. ENGLE: Can I interrupt, and just say, I
23 was not speaking for the FTC --

24 MS. DELANEY: It's too late.

25 (Laughter.)

1 MS. ENGLE: -- or any individual commissioner,
2 or the FTC staff.

3 MS. BAIRD: Well, I think that the answer to
4 that question is kind of a sub-section under the general
5 Spyware problem, and that gets back to what I was saying
6 earlier. You -- it's hard to prove that there's been any
7 harm or wrong, if, for example, someone's computer has
8 just slowed down, or if they, you know, have to wipe off
9 everything that's on their computer and start all over.
10 You know, that's -- there's not any monetary damage
11 there, and there isn't any -- any personally-identifiable
12 information per se that has been taken because of it.

13 However, the Congresswoman would argue that
14 that is, in fact, damage, and that that should be
15 included under Section 5-A of the FTC Act, as an unfair
16 deceptive act, since the consumer, when he or she
17 downloaded it, had no idea that by downloading it, they
18 would cause such things to happen to their computer. And
19 if course, you know, no notice is going to say "If you
20 download this, it might slow down your computer,"
21 however, it will say "This is what the purpose of this
22 software is. This is it's function, this is what it will
23 collect, and this is what we will do with it."

24 And so, the idea is -- and you know, it's
25 surprising to hear what Matthew says, but I believe it.

1 I believe that there are some people who actually would
2 continue with the downloading process. That's why my
3 boss doesn't necessarily say that Spyware should be
4 prohibited, but instead, consumers should have the choice
5 to decide whether or not they want to download it. And
6 when they make that decision, they should have -- they
7 should be informed as to what they are deciding.

8 And, of course, as I mentioned before, this --
9 this requires a combination of legislative action, as
10 well as self regulation and industry, and just, you know,
11 consumer education in general by all entities interested
12 and involved in Spyware.

13 MS. DELANEY: "Representative Urquhart, your
14 bill exempts operating systems from the definition of
15 Spyware. As you are probably aware, there has been a lot
16 of litigation about what is bundled, or integrated into a
17 dominant operating system. Is it your understanding that
18 an application that is bundled, integrated into the
19 dominant operating system is not covered -- for example,
20 Windows Media Player, while others, for example, Real
21 Player or Apple Quick Time, would be covered?"

22 MR. URQUHART: Yeah, let me point out that, in
23 Utah, like in most states, we don't write our laws into -
24 - in stone. We don't chisel them in stone, we write them
25 on paper, and so, we have made it plenty clear to

1 industry, and to all parties, that we wanted their input.
2 And about the only input we got during the sessions was,
3 don't do it. Let -- for Heaven's sake, let the feds deal
4 with this, and, you know, that -- that's not acceptable
5 to my consumers. And so, this was brought forward by an
6 industry member, saying put in an operating system, and
7 currently, in the law, they could argue that this is a
8 vital component of the operating system, then it would be
9 exempted out.

10 But, you know, if someone were wanting to make
11 the case, then they could go through all the detailed
12 criteria, stating otherwise, that it does monitor
13 activity, that it sends information about the -- the
14 computer use, it doesn't provide adequate disclosures,
15 and it's not easily removable. So, you know, to answer
16 your question, I -- I think currently, the way the law is
17 written, those would not be covered by the law.

18 MS. DELANEY: Okay. I have another question,
19 here. I think you did touch on this, but I'll -- I'll
20 ask it, and you can have an abbreviated answer if it's
21 been fully covered. "How are, for example, Utah contact
22 lens consumers harmed by receiving a point of purchase
23 pop-up from another vendor with lower prices on the same
24 item?"

25 MR. URQUHART: Well, again, if you could

1 guarantee that it were lower prices, that would be a
2 different issue, but there's no guarantee there what's
3 going is -- in the case of contact lenses, again, you
4 have someone with stuff on their computer, and they're
5 just bombarded by advertisements. No one says that it is
6 a better deal. It's just stuff that they didn't consent
7 to have it there, and so, it just keeps popping up, and
8 they should have a say. So again, it goes back to
9 consent.

10 They're -- they're harmed by the fact that it
11 is using up the resources of their machine, and then the
12 contact lens company would also be harmed, if it came on,
13 and someone was just triggering off their site, they've
14 spent all the money to invest in that site. Maybe an
15 affiliated marketer has pushed someone to that site, they
16 also have invested, and so then, if, at the point of
17 purchase, someone pops right in, well, there's very
18 little investment that went into that. And that's why
19 the profits of these Adware companies -- the profit
20 margin is just unbelievable. I mean, the only comparable
21 thing with a similar profit margin is crime. You know,
22 one crow bar, and -- and you're in business.

23 And so, here that -- that again is my point,
24 that if we allow this conduct to happen, then all efforts
25 are pushed just to the harvest, and not to actually

1 building the business.

2 MS. DELANEY: And then, I think we have time
3 for one more question. This one is for Mark. Although,
4 Representative Urquhart, you, by far, have the most
5 questions. But I'll spare you. Mark, "If a user is
6 unaware that a software application is running on their
7 PC, can it still be argued that they have agreed to the
8 license agreement?"

9 MR. ECKENWILER: As a lawyer, I can tell you
10 that anything can be argued. And, in fact, that's --
11 that's one of the -- one of the challenges in this area,
12 I think. I -- I don't -- I don't want to be on record, I
13 actually agree with Mary that I -- I don't think my
14 position -- since I don't speak for the Department of
15 Justice, the U.S. government, or Major League Baseball
16 here today, is that no legislation in this area is at all
17 appropriate.

18 I think the point is well taken that, if we
19 were to try to charge somebody with, you know, a Computer
20 Fraud and Abuse Act violation for putting up -- you know,
21 one of these "Do you want to accept this" screens that's,
22 you know, 25 pages long in six-point type, in a very
23 narrow column, totally unreadable, it's not the most
24 attractive circumstance for us to bring a criminal
25 prosecution, remembering that we actually have a

1 Constitutional burden to prove beyond a reasonable doubt
2 that, as I said before, this was under 1030, without or
3 in excess of authorization.

4 I think the first line of defense in such a
5 case is going to be that the defendant was, in fact,
6 acting within the scope of authorization, and that
7 becomes a kind of ugly jury question. If we're going to
8 pick and choose cases to prosecute, I think we are more
9 likely to take cases like the Jon case, or this newly-
10 indicted case, the Ropp case, where there just -- there's
11 no argument that that was -- there was never any
12 constructive notice. Never even any attempt at notice.
13 This was, you know, purely a -- a clandestine
14 installation.

15 So, yeah, it could be argued, it -- it's -- it
16 is certainly a consideration, deciding whether or not to
17 -- to bring a case.

18 MR. SARREL: Hey, I wonder if you could just
19 ask the jury if they've ever read a license agreement.

20 MS. ENGLE: And can I just follow up on that
21 from -- from our perspective. The FTC law is pretty
22 clear that, if you're going to give notice to consumers
23 of something, it has to be clear and conspicuous, and we
24 have actually issued a long -- you know, several years
25 ago now, guidance to the online community called "Dot Com

1 Disclosure," that gives you a pretty good understanding
2 of how to make disclosures clear and conspicuous to
3 consumers, and that includes things like, if they've got
4 to click on a button to find out the information, that
5 the button has to be clearly labeled, and also, labeled
6 with the import, so that they know why they should be
7 clicking, not -- not just click here for more info, or
8 something like that. So, from our perspective, just
9 because some term is buried in a four-page ULA doesn't
10 mean that consumers have necessarily given their consent
11 to it.

12 MS. DELANEY: Great. Does anybody else have
13 anything to add before we finish up? I'd like to ask
14 everyone in the audience just to stay seated for a
15 moment. We're going to have closing remarks from
16 Director Beales. I think -- the panelists, can we sit
17 down, or should we stand here? I think panelists can go
18 back to their seats, but if everyone in the audience
19 could remain seated.

20 (Applause.)

21 MR. PAHL: Well, thanks, Beth, and -- and to
22 the members of our Government Response panel. The last,
23 but certainly not least part of our program today is some
24 closing remarks by BCP director, Howard Beales. Howard?

25 MR. BEALES: Thanks, Tom, and -- and thanks to

1 all of you for sticking around. We've reached the end of
2 an important, and, I think, productive workshop. I want
3 to thank all of the panelists who volunteered their time
4 and expertise to discuss the varied and complex issues
5 related to Spyware.

6 I'd like to thank those of you who were not
7 panelists, but who provided public comments, or posed
8 questions to direct our discussions, and helped us to
9 build a rich and detailed record. The record remains
10 open for public comments until May 21st. Please use this
11 opportunity to submit a comment in response to what
12 you've heard today. The instructions for submitting a
13 comment are on the FTC Spyware Workshop web page, that's
14 FTC.gov/bcp/workshop/spyware.

15 I particularly wanted to thank Commissioner
16 Swindle and Commission Thompson for participating in the
17 workshop. Their leadership has been, and will continue
18 to be, critical, as the commission assesses what is
19 Spyware, what problems it might cause, and the merits of
20 possible solutions to these problems. And last, but
21 certainly not least, I'd really like to thank the staff
22 of the Division of Advertising Practices for their
23 exemplary work in organizing this workshop.

24 The panels this morning were a spirited and
25 informative discussion that will give us a better

1 understanding of what Spyware is, and the problems that
2 Spyware may cause. This afternoon, we heard a vigorous
3 debate about the many options available to the
4 government, to industry, and to consumers, to respond to
5 Spyware. Today's discussions will provide important
6 grist for the mill as we consider possible responses to
7 the issues that Spyware raises.

8 Let me offer some thoughts based on what I've
9 heard today. It seems clear from today's discussions
10 that there is software that may cause privacy, security,
11 and functionality problems for consumers. The FTC's
12 privacy agenda focuses on the misuse of consumer
13 information, and the explicit recognition of trade-offs
14 in our information economy. But consumers may not
15 understand the trade-offs related to Spyware.

16 Spyware may harvest personally-identifiable
17 information through monitoring computer use, without
18 their consent. It may also facilitate identity theft by
19 surreptitiously planting a keystroke logger on a user's
20 personal computer. It may create security risks, if it
21 exposes communication channels to hackers. It may also
22 affect the operation of personal computers, causing
23 crashes, browser hijackings, home page resettings, and
24 the like. These harms are problems in themselves, and
25 could lead to a loss of consumer confidence in the

1 Internet as a means of communication and confidence. And
2 in commerce.

3 Second, many of the panelists discussed how
4 Spyware may cause problems for business, too. Companies
5 may incur costs as they seek to block Spyware from the
6 computers of their employees. Employees will be less
7 productive if Spyware causes their computers to crash, or
8 they're distracted from their tasks by a barrage of pop-
9 up ads. Spyware that captures the keystrokes of
10 employees could be used to obtain trade secrets, and
11 other confidential information from businesses.

12 Because of the novelty of Spyware, there's been
13 little empirical data as to the prevalence and magnitude
14 of these problems, for consumers or businesses. But some
15 of the potential risks are severe, and government,
16 industry and consumers should take steps to keep these
17 problems from spreading. Fortunately, we hear this
18 afternoon that substantial efforts are currently underway
19 to address Spyware. In response to market forces,
20 industry is developing and deploying new technologies to
21 assist consumers.

22 Consumers and businesses are becoming more
23 aware of the risks of Spyware, and they're responding by
24 installing anti-Spyware products, and other measures.
25 Today, certain industry representatives indicated that

1 they would explore best practices and consumer education
2 on issues related to Spyware. Government and industry-
3 sponsored education programs, and industry self
4 regulation, could be instrumental in making users aware -
5 - or more aware -- of the risks of Spyware, thereby
6 assisting them in taking actions to protect themselves.

7 These approaches let consumers choose the
8 trade-offs that work for them. I think that all of these
9 efforts are very encouraging. Although there are several
10 efforts underway to address the issues and concerns
11 created by Spyware, we must take -- we must carefully and
12 clearly define the problem. Spyware is an elastic and
13 vague term that has -- that it has been, and could be,
14 used to describe a wide range of software.

15 A vague definition of Spyware could be so broad
16 that it covers software that's beneficial, or benign,
17 software that is harmful, software that is beneficial or
18 benign but misused, and software that is just poorly
19 written, or inefficient code. Such imprecise definitions
20 would treat these types of software in the same manner.
21 We need to determine whether there is a definable class
22 of software that can truly be called Spyware.

23 The easiest way to start drawing lines is case-
24 by-case law enforcement. We have had investigations in
25 this area, and we will have more. But we need your help.

1 When you see bad practices, please tell us. And please
2 tell us whatever you know about who is engaged in these
3 bad practices. We're taking names.

4 This workshop has generated a tremendous amount
5 of information for the commission, and for the public to
6 evaluate, relating to Spyware. I'm confident that the
7 workshop will assist government, business, and consumers
8 in developing effective and properly-focused responses to
9 Spyware. Thank you again for coming, and for devoting
10 your time and effort to making this workshop happen.
11 Thank you.

12 (Applause.)

13 (Whereupon, at 5:51 p.m., the workshop was
14 concluded.)

15 * * * * *

16

17

18

19

20

21

22

23

24

25

