AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

# SPYWARE: WHAT YOU DON'T KNOW CAN HURT YOU

## HEARING

BEFORE THE

SUBCOMMITTEE ON
COMMERCE, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

APRIL 29, 2004

**Serial No. 108–89**

Printed for the use of the Committee on Energy and Commerce

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE

93–308PDF WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

## COMMITTEE ON ENERGY AND COMMERCE

JOE BARTON, Texas, Chairman

W.J. "BILLY" TAUZIN, Louisiana
RALPH M. HALL, Texas
MICHAEL BILIRAKIS, Florida
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
RICHARD BURR, North Carolina
ED WHITFIELD, Kentucky
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi, *Vice Chairman*
VITO FOSSELLA, New York
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
DARRELL E. ISSA, California
C.L. "BUTCH" OTTER, Idaho
JOHN SULLIVAN, Oklahoma

JOHN D. DINGELL, Michigan
*Ranking Member*
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN McCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DeGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
TOM ALLEN, Maine
JIM DAVIS, Florida
JANICE D. SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas

BUD ALBRIGHT, *Staff Director*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

---

## SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

CLIFF STEARNS, Florida, *Chairman*

FRED UPTON, Michigan
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
*Vice Chairman*
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
DARRELL E. ISSA, California
C.L. "BUTCH" OTTER, Idaho
JOHN SULLIVAN, Oklahoma
JOE BARTON, Texas,
(Ex Officio)

JANICE D. SCHAKOWSKY, Illinois
*Ranking Member*
CHARLES A. GONZALEZ, Texas
EDOLPHUS TOWNS, New York
SHERROD BROWN, Ohio
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
BART STUPAK, Michigan
GENE GREEN, Texas
KAREN McCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DeGETTE, Colorado
JIM DAVIS, Florida
JOHN D. DINGELL, Michigan,
(Ex Officio)

# CONTENTS


| | Page |
|---|---|
| Testimony of: | |
| Baker, David N., Vice President, Law and Public Policy, Earthlink | 36 |
| Beales, J. Howard, III, Director, Bureau of Consumer Protection, Federal Trade Commission | 42 |
| Friedberg, Jeffrey, Director of Windows Privacy, Microsoft | 10 |
| Schwartz, Ari, Associate Director, Center for Democracy and Technology | 47 |
| Thompson, Hon. Mozelle W., Commissioner, Federal Trade Commission | 38 |
| Additional material submitted for the record: | |
| Downloading Shared Files Threatens Security, article by Sgt. 1st Class Eric North | 86 |
| Thompson, Roger, Vice President for Product Development, PestPatrol, Inc., prepared statement of | 81 |
| Webroot Software, Inc., prepared statement of | 83 |

# SPYWARE: WHAT YOU DON'T KNOW CAN HURT YOU

**THURSDAY, APRIL 29, 2004**

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON COMMERCE, TRADE,
AND CONSUMER PROTECTION,
*Washington, DC.*

The subcommittee met, pursuant to notice, at 10 a.m., in room 2123, Rayburn House Office Building, Hon. Cliff Stearns (chairman) presiding.

Members present: Representatives Stearns, Upton, Shimkus, Shadegg, Bass, Bono, Otter, Barton (ex officio), Schakowsky, and Strickland.

Alsp present: Representatives Inslee and Greenwood.

Staff present: David L. Cavicke, majority counsel; Chris Leahy, policy coordinator; Shannon Jacquot, majority counsel; Brian McCullough, majority professional staff; Jill Latham, legislative clerk; William Carty, legislative clerk; and Consuela Washington, minority counsel.

Mr. STEARNS. Good morning. I am pleased to welcome all of you to the Commerce, Trade and Consumer Protection Subcommittee hearing on spyware. Spyware is loosely defined as malicious software, downloaded from the internet that spies on the computer owner or user, usually to provide information to third parties. The Federal Trade Commission has said that spyware is software, that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent or that assert control over a computer without the consumer's knowledge. A spyware relative, known as adware, enables the computer owner or user to receive a stream of ads and other marketing information usually based on data the software has collected about the user. Adware or ad supported software is frequently bundled with free internet software or free ware. Legitimate adware allows the user knowledge and consent about the software and frequently provides an adware free version for purchase. More noxious adware versions, however, can be downloaded without consent or through deceptive means, essentially making them spyware in themselves.

My colleagues, as we speak, spyware and adware software programs are growing at a very, very rapid rate. According to the consumer security firm, McAfee, these software programs have grown in number from about 2 million in August 2003 to over 14 million currently.

As further proof of the potential scale of this problem, the National Cyber Security Alliance has estimated that over 90 percent of users had some form of adware or software, spyware on their computers and yet, most were unaware of it. In worse cases, the more malicious varieties of spyware can record keystrokes and compromise personal information, including passwords and Social Security Numbers.

The simple act of downloading a desired program from the internet can not only open the door on your personal computer and your most private information, but also can allow spies to effectively take up resident in your personal computer. Your personal property, I might add, without your knowledge and without your consent.

Then after sneaking into your computer, some of these malicious spyware programs can act as snoop, prying into your private life or thieves, stealing personal information or as pornography dealers, exposing your children to obscene online material.

If and when you finally discover the spy lurking in your personal computer, the damage is already done. In the best cases, the technology that enables spyware also can serve as a first line of defense against obscene internet material by tracking website activity and filtering out the garbage. Other forms of the technology, like legitimate adware, are authorized by the consumer and provides businesses a new and efficient means of reaching potential customers with less expensive goods and services.

While some would have us to find spyware with technical parameters, others believe that it is not the technology tool that needs to be defined and targeted. It's the unscrupulous individuals preying on the consumer from these programs.

Clearly, no matter the definition we create today, it is always reprehensible when someone intentionally downloads secret software into a personal computer that is designed to steal information or trick us into opening the doors into our private lives.

To try to address this egregious internet activity, Ms. Bono of California, has introduced legislation to enhance spyware disclosures, root out this deceptive and fraudulent and create accountability. Her bill require the computer users receive clear and conspicuous notice prior to downloading spyware and that all third parties provide their identity.

I sincerely commend her for her leadership on this issue. It is my hope that we can reach bipartisan consensus on legislation that will protect consumers from unwittingly being spied upon.

With the help of our distinguished panel of witnesses, one of our most important tasks is to try to establish the boundaries of what is clearly legitimate and what is clearly reprehensible. We then need to explore the murky area in the middle where cases aren't so stark and are not so clear-cut, especially in cases where consumers are duped with lengthy and confusing license agreements, website trickery and exploitation of weak, personal computer security.

The ultimate challenge, therefore, is to investigate ways industry, consumers and Congress can work together to rid out our online marketplace of the bad apples, while preserving legitimate uses for this software technology.

And finally, my colleagues, our panel today will help us understand how spyware and adware programs are distributed in commerce, both legitimate and fraudulent. The scope of the privacy and security risk posed by this software, its effects on economic productivity and the need for Federal legislation. And I think many of you know that the State of Utah has already passed a spyware bill. The State of California and New York are presently looking at that.

I welcome our witnesses today and I look forward to their testimony and with that, I call on the ranking member for her opening statement.

Ms. SCHAKOWSKY. Thank you, Chairman Stearns. One of the great things about this job is that you learn something new every day. So that either indicates that I am way behind the curve here or that perhaps the Congress is getting a grip on an emerging problem. Because increasingly people are finding that their home web pages are changed or their computers are sluggish, we get pop up ads that won't go away no matter how many times they try to close them. They find software on their computer they didn't install and they can't uninstall. Their computers are no longer their own and they can't figure out why.

They think that the problem is with their computer, with a program they installed or with their internet service provider, but more and more often, it's becoming clear that they are the unwitting victims of spyware. Because they clicked on the wrong web page or signed an agreement to download one program, spyware has made it on to their computer.

While the above examples can be written off by some as merely annoying, there are serious privacy and security issues at stake. The tracking capability of spyware programs can be so powerful that it can record every keystroke computer users enter. It can take pictures of personal computer screens. It can snatch personal information from consumers' hard drives. People can see their bank account numbers, passwords and other personal information stolen because they quite innocently went to a bad website or clicked an agreement they didn't know they shouldn't.

While some programs called spyware can have legitimate purposes like allowing for access to online newspapers without having to register every time you want to read it, truly nefarious spyware uses software and applications in ways that cannot be defended. Spyware purveyors engaged in unfair and deceptive practices. They take personal information without permission. They exploit software vulnerabilities and co-op'd others' computers.

Fortunately, we do have a number of laws on the books that we can use against spyware. However, there has been virtually no enforcement of the laws. Spyware transmitters know how to cover their tracks and technology changes every day. It makes it very hard to find those who are to blame, but it can be done and we need to pursue enforcement of laws already on the books.

And we also need to explore legislation and other responses to deal with the inevitable loopholes that exist in the law because of the ever-evolving nature of technology. That's why I'm glad we're here and glad I'm here today to start discussing the best way we as legislators can address these issues.

We also need to get the word out to consumers so that they know what is really wrong with their computers and so that they can protect themselves from online predators. We should build on the consumer awareness efforts of the FTC and Center for Democracy and Technology as a right of their pursuing comments about how spyware has affected people. They have heard from hundreds of consumers concerned about spyware's invasion into their privacy. From these comments and very technical investigative follow-up, the Center for Democracy and Technology has filed complaints with the FTC about two spyware bad actors. I'm quite pleased that we have distinguished witnesses representing the broad spectrum of affected parties and as Chairman Stearns mentioned, we have the industry regulators and consumer groups and I look forward to hearing from all of you.

Thank you.

Mr. STEARNS. I thank my colleague. The distinguished chairman of the full committee, the gentleman from Texas, Mr. Barton.

Chairman BARTON. Well, thank you, Chairman Stearns, for holding this hearing and I want to thank Congresswoman Bono for introducing this piece of legislation.

We checked our committee computers this week and found 167 spyware programs on it. I told that at a meeting breakfast a couple of days ago and the gentleman held up his hand and said he had just checked his computer and had over 200 and then I told the story at dinner last night and somebody held up their hand and said over 400. So there is no more pernicious, intrusive activity going on on the internet today than the subject of this hearing. And I hope that after the hearing, we can come together on a bipartisan basis and decide what to do legislatively about it.

I have told Congresswoman Bono that her bill is a starting point, but not the end point and I want to tell all of the members of the committee and the folks in the audience and the people that are watching this on television, if it's being broadcast, that we really intend to do something about this. We do not let people just wander around our homes without our permission. We don't let total strangers just come up to us, encourage us to buy this or buy that or do this or do that. And we certainly when we have guests over, and they overstay their welcome, we encourage them to leave. None of those can we do with these spyware programs that are proliferating on our personal computers and as we found out at the committee this week, our office computers.

So I am very, very pleased that Chairman Stearns is holding this hearing and I am very, very hopeful that after the record is developed from this hearing that we can very quickly move to a legislative solution to that to cure this cancer on the internet.

And with that, Mr. Chairman, I have an official statement for the record, but I will yield my time back.

Mr. STEARNS. By unanimous consent, so ordered.

Chairman BARTON. Thank you.

[The prepared statement of Hon. Joe Barton follows:]

PREPARED STATEMENT OF HON. JOE BARTON, CHAIRMAN, COMMITTEE ON ENERGY AND COMMERCE

Thank you, Mr. Chairman, for holding this hearing today. It continues this Committee's longstanding work in the area of consumer protection.

Spyware may be unfamiliar to many Americans, but unfamiliar does not mean unaffected. I suspect a large number of those in this room are victims of some of these foul abuses. Certainly all of us who use the Internet are threatened by them. And the very nature of the abuse is what keeps everyone threatened by it from seeking relief. It is aptly named spyware. Its installation is often sneaky or deceptive and even when it runs it often goes undetected. And when consumers notice related problems with their systems, those problems are easy to misdiagnose. Even those that are technically savvy and aware of what is on their system, may not be able to uninstall spyware.

Much of the recent discussion surrounding spyware has focused on the difficulty in defining what it is. The most pernicious of the software is composed of keystroke loggers and screen-capture utilities. This has both privacy and security issues for consumer Internet use. For example, some software can pick up your sensitive financial information when you use on-line banking, or it could monitor your email traffic and transmit personal information contained in that email. Both could lead to identity theft and other privacy and security abuses.

There is also "adware." While adware does not capture keystrokes it often captures information, like websites visited, and sends that information back to a central server for the purpose of delivering targeted advertising. I would be suspicious of someone following me around the shopping mall and popping over to me and offering me a better deal each time I reached a register. I suspect most of us would call the police. But this adware does the very same thing. It follows you around the Internet and just as you are looking at purchases, it invades your computer with related and often unrelated offers. There may be some who would consent to this "point of sale" availability of information. It is certainly marketing genius. But, without informed consent, it is a true invasion of privacy.

We ran a sweep of a Committee computer earlier this week and discovered there were over 167 "hits" for third party cookies and adware. A recent demonstration by an anti-spyware software company showed that most of that software ended up on the computer just by visiting a site. No consent was requested and none was given. If I want someone to come into my home I invite them into my home—if they come in uninvited that is a trespass. And certainly if they take something from inside without authorization it is a burglary. The same should hold true for access to my home and information via my computer.

The Internet has been a great boon to society as a tool for information and commerce. But, surfing the web is increasingly becoming a defensive exercise for consumers who wish to protect their privacy and maintain the security of their information. If this dynamic does not change soon, there is a real risk of undermining all the commercial gains the Internet has achieved.I thank our witnesses for their participation today and look forward to their testimony. In particular, I would like to thank Ms. Bono and Mr. Towns for their leadership in introducing legislation to enhance disclosures to consumers concerning spyware. After this hearing I will be working with all Members of the Committee on a legislative solution to this problem.

Thank you and I yield back.

Mr. STEARNS. And I thank the distinguished chairman and at this point we'll have the author of the bill, the gentlelady from California for an opening statement.

Ms. BONO. Thank you, Chairman Stearns, and Chairman Barton for your leadership on this issue. I welcome the full weight of the committee chairman and subcommittee chairman behind this legislation. It's also been a pleasure to work with Congressman Ed Towns who apparently caught a flight home today.

We introduced H.R. 2929. We called it the Safeguards Against Privacy Invasions Act. I look forward to hearing from all of our witnesses this morning.

Spyware is a technological disease that is proliferating each day. It threatens the efficiency of our computers and internet services as well as the security of our personal information and private transactions. Spyware programs can secretly hijack web browsers and collect web surfing patterns, keystrokes, password information, all that without the computer user ever knowing that it has even occurred.

In fact, more often than not, computer users have no idea that they have downloaded spyware, nor do they have any idea as to how they obtained it. Yesterday, Harris Interactive released a web at work study which discovered that 92 percent of information technology managers estimate that their organizations have been infected by spyware at some point. However, only approximately 6 percent of the employees who access the internet at work say they have ever visited websites that contain spyware.

EarthLink and Webroot Software recently scanned more than 1 million personal computers and reported 23.8 million cookies and approximately 5.7 million adware and spyware programs. Pest Patrol which sells its own spyware remover, estimates that there are more than 78,000 lurking spyware programs. One of the main conduits for the spyware industry is the peer to peer file sharing scheme. Free file sharing services like Grokster and Kazaa which are also centers for illegal copying, usually tie several pieces of adware and spyware to their programs. Kazaa, for example, bundles Gator with its software. Gator, in turn, contracts with companies who want targeted advertisements. For a fee, Gator agrees to disseminate its software so that internet habits can be monitored enabling targeted advertisements.

However, spyware is not limited to bundling with other software programs such as Kazaa. In fact, some websites and e-mail messages trick computer users into downloading spyware. One common trick is to alert the computer user that his or her system is vulnerable and he or she must immediately download a security patch. However, the patch only turns out to be spyware or adware. Spyware affects everyone from the most tech savvy computer users to the least tech savvy computer users and certainly unsuspecting teens and kids.

Lynn Vaccaro, a manager at Errol Electronics, one of the largest distributors of computer products, was having difficulty with pop up ads, so she tried different pop up stoppers with no avail. She then realized she had spyware on her computer. She download SpyBot Search and Destroy and many other scanner and removal tools. The tools worked so well that they eliminated parts of Internet Explorer as well as Windows. She then had to reload both of them.

H.R. 2929 would require that spyware companies give clear, concise and conspicuous notice to computer users about the function of their software as well as the information that may be collected and transmitted through their software. After giving such notice, the computer user would have to agree to the downloading of the software. In other words, under the SPI Act, spyware would no longer be used to spy on unsuspecting computer users.

Although Congress has a responsibility to address the issues surrounding spyware, it is equally imperative that the Federal Trade Commission, as well as the technology industry, does all that it can to protect consumers from spyware. Moreover, it is necessary that we collectively educate consumers about the nature and the threats of spyware.

I hope this hearing will help all of us learn more about spyware and it will enable us to begin tackling some of the complicated and technical questions that are related to spyware.

Thank you, Mr. Chairman.

Mr. STEARNS. I thank the gentlelady. Mr. Shimkus.

Mr. SHIMKUS. Thank you, Mr. Chairman. I'll be brief. I bought a new Dell. I got Windows XP. I'm disappointed with both of those. My computer is lots more sluggish than it ever was under my own system that had less memory, less capabilities and it's unfortunate and I think it's because I've got programs competing with each other. It's like trying to ride an old Western, you're on that stagecoach and you've got those 16 horses and you've got both reins and you just can't control it. It's tremendously frustrating and I'm not tech savvy at all.

So this one of many issues that I think is frustrating the public and I'm glad Mary has seen fit to work Mr. Towns and really address this. This hearing is very, very important.

This also gives me the opportunity because of the inability to control our own personal computers any more. It also gives me the chance to advertise once again for .kids.us, the importance of that, if you want to protect kids on the internet and we have a late weekend sale, we're having our hearing. I think next week, Thursday, maybe, so those of you who have not got a site up on .kids.us, you still have time before we have the hearing and start identifying those good entities that are trying to protect kids and those who are still a little negligent and we will continue to try to coerce them.

I did receive an e-mail, Mr. Chairman, if I may submit into the record.

Mr. STEARNS. By unanimous consent, so ordered.

Mr. SHIMKUS. It's from Sergeant First Class on peer to peer issues and it's probably well known in the community. The other issue to this debate is the threat to national security. If these things are on Department of Defense computers and individuals have the ability then to snoop around in our intelligence community, Department of Defense, FBI and the like, this is a really serious national security concern. I think this article highlights that and so I think this is a very timely hearing. I thank you for calling it and I thank my colleague, Mary Bono, for bringing it to our attention.

I yield back.

Mr. STEARNS. I thank the gentleman. The gentleman from Michigan, Mr. Upton.

Mr. UPTON. Well, thank you, Mr. Chairman. I want to thank my colleague, Ms. Bono, as well, for the great work she's done on this legislation. I might say that I've got a Dell as well at home with an XP in it. At the beginning when you turn it on, I used to make a joke with my kids there's a lot of little guys inside, the click, click and they run around trying to plug in the old circuits, sort of like the old telephone, but now it's—you need Raid because you find out, in fact, it's not little guys in there. It's spiders. And I've been a victim of spyware as well. I don't know how many hundred, Mr. Barton, that I have, but I have a 12-year-old and a 16-year-old and we had to have the computer doctor come visit and take it away and take it to the ER and it's on life support. Found out it couldn't even deal a deck of cards in Solitaire it was so slow, it was so pathetic. It's bad. It is bad.

I think for a lot of Americans when they become victims of this they're a little surprised and they become very alarmed and then they become very angry and bitter that someone would violate their personal space whether it be Kazaa or anybody else and in fact, victimized an entire family, homework and everything else, that a PC provides assistance with.

So I think that we need legislation on this. I think we need strong penalties. Some might suggest the death penalty. I don't know that we'll go that far, we'll look for some judiciary help, but I want to thank my colleague, Ms. Bono, for this. I want to thank you, Mr. Chairman, for holding this hearing and hopefully, we will move on a strong bipartisan basis to use the Raid to get those little guys out of there.

I yield back my time.

Mr. STEARNS. I thank the gentleman. The gentleman from New Hampshire, Mr. Bass.

Mr. BASS. Thank you, Mr. Chairman, a great hearing. I've all the same issues that everybody else has talked today. I'm eager to hear the witnesses, so I yield back.

Mr. STEARNS. I thank the gentleman. Mr. Otter?

Mr. OTTER. Well, thank you, Mr. Chairman, and let me join in this core of folks in showing appreciation to Ms. Bono for her efforts on bringing this to our attention and also holding this hearing and getting some sort of a resolve.

Over the last few years, this Congress has debated the privacy issues on many fronts. The passage of the Health Insurance Portability and Accountability Act, created new privacy protection for individuals in the health market. However, Congress also passed the Patriot Act which has caused many, including myself, to carefully evaluate the value we place on personal privacy. I believe many in the public are not aware of the many ways they are being watched online, tracked online and in recent years there have been an increased awareness of identity theft, yet we still hear little about the intrusiveness and the risk associated with spyware.

There's no doubt that the function of spyware is to watch, to track, record an individual's internet usage and activity, often without the knowledge of the user. I'm very interested in hearing from the witnesses today on what they believe is an appropriate way to notify users before they download spyware.

I'm also very concerned about the websites like Kazaa that infect computers with spyware in exchange for providing user access to stolen goods and then profit from them by selling the information collected by spyware to other advertisers. As an advocate of personal responsibility, I also believe that users who participate in these illegal activities on these sites such as music and movie theft, should expect to be taken advantage of and I have little sympathy for them.

If you're going to play with fire, you need to expect to get burned. So if you don't want spyware from Kazaa and other similar sites on your computer, don't participate in these illegal activities.

Mr. Chairman, once again, I thank you and I thank Ms. Bono for the opportunity to examine these issues and look for solutions in solving them. I yield back.

Mr. STEARNS. I thank the gentleman and just for his information, we're going to have a hearing on this Kazaa and the peer to peer later.

The gentleman from Arizona, Mr. Shadegg.

Mr. SHADEGG. Thank you, Mr. Chairman, I am also anxious to hear the witnesses because I think this is an extremely important topic. I similarly want to congratulate our colleague from California, Ms. Bono, on bringing an important issue to the committee. I think this is an issue that we need to be very attentive to and quite frankly, it's an area where I think we need legislation. I want to compliment you on holding the hearing.

Mr. STEARNS. I thank the gentleman. We also welcome Mr. Inslee from the State of Washington. He is a guest here with the committee.

[Additional statement submitted for the record follows:]

PREPARED STATEMENT OF HON. BARBARA CUBIN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WYOMING

Thank you, Mr. Chairman, for holding this timely hearing.

I would also like to thank the distinguished panel of witnesses here today. Today's hearing brings together an assembly of panelists who are recognized experts of various technological industries, and I anticipate their insights to be of unparalleled value as we delve into the issues surrounding spyware.

As Americans become increasingly dependent upon computer technology to navigate everyday life, there is a consumer-driven demand for technology to be perpetually updated. Unfortunately, in the continuously expanding domain of computer technology, there also exists the knowledge to utilize software for less desirable results. Today's hearing will educate and warn us all of an emerging, largely undesirable software technology phenomena known as spyware.

Today's hearing will foster debate and thought regarding several complex issues surrounding spyware. First and perhaps most gravely is the need to develop a clear and accepted definition of spyware. We must first acknowledge that instances where this type of software can be used by third parties for valid and useful purposes do in fact exist. However, it is when this technology is utilized by unethical and fraudulent purposes that alarm must be raised. While most Americans will never understand how spyware is engineered, it is indisputably unacceptable for someone to secretly download software onto another's computer with the intent of stealing personal information. Therefore, today's debate should be based upon the bad practices and deviant behavior of promulgators of spyware rather than its technological aspects.

Aside from the need to apply a definition to spyware, there also exists a need to examine the more complex matter of enforcing punishment of the inappropriate use of this technology. While consumers may not object to receiving advertisements, a line that must be drawn before people are allowed to use spyware for more invasive and intrusive purposes. Today's hearing will reveal what steps software industry leaders are taking to protect consumers from such invasions and increase our understanding of what role Congress should play in this capacity.

Most importantly, today we have the opportuniy to help raise consumer awareness of the increasingly dangerous use of spyware. The majority of American consumers have likely been affected by spyware at some level, and I foresee today's hearing as the embarkment of a large-scale campaign to help Americans better educate and protect themselves from the inappropriate use of spyware.

Thank you Chairman, and I yield back the balance of my time.

Mr. STEARNS. We're going to, since the opening statements are complete, we're going to depart from the normal schedule and hearing from the witnesses. We're going to go to a demonstration. I would hope that we would have an actual demonstration of how spyware is used and so with that further ado, we'll have this demonstration.

Mr. FRIEDBERG. Actually, it's going to be part of my testimony, so I can do it all at once.

Mr. STEARNS. We'll let you start and go ahead and do that then.

**STATEMENTS OF JEFFREY FRIEDBERG, DIRECTOR OF WINDOWS PRIVACY, MICROSOFT; DAVID N. BAKER, VICE PRESIDENT, LAW AND PUBLIC POLICY, EARTHLINK; HON. MOZELLE W. THOMPSON, COMMISSIONER, FEDERAL TRADE COMMISSION; J. HOWARD BEALES III, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION; AND ARI SCHWARTZ, ASSOCIATE DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY**

Mr. FRIEDBERG. Great. Chairman Stearns, Ranking Member Schakowsky and members of the subcommittee, my name is Jeffrey Friedberg and I am the Director of Windows Privacy at Microsoft Corporation. Thank you for the opportunity to share our views on this growing threat to computer users around the world. I'd like to comment the subcommittee for holding this hearing and its bipartisan approach to this important consumer issue.

I'd also like to acknowledge Representatives Bono and Towns for the time and energy they have invested.

Spyware and deceptive software share a common theme. They use ambiguity, coercion, deceit and outright trickery to lure and even force users to execute or install unwanted programs. They can be invasive, offensive and even destructive.

Our customers complaint that deceptive software degrades their computing experiences, in some cases, making their computers unusable. We have evidence that this software is at least partially responsible for approximately half of the application crashes our customers report to us. It has become a multi-million dollar support issue for computer manufacturers, ISPs and companies like Microsoft.

I'm going to show you some examples of how our customers have been tricked. My first slide illustrates what we call a pop-under exploit. We don't have it on the back screen at the moment.

Chairman BARTON. I think we have spyware infecting our application here.

Mr. FRIEDBERG. Great.

Mr. STEARNS. Do you just want to turn down the lights a little bit? Is that possible to do that?

Mr. FRIEDBERG. So in this case a user goes to a website they trust. I've simulated a news website here, may be their favorite site, and after a delay——

Mr. STEARNS. Just pull the mic up a little bit more because when you turn your head, we lose you.

Mr. FRIEDBERG. Sorry. And after a delay, they get the security warning which is normal which says hey, somebody is trying to download software to you. Now the user thinks this might be coming from the trusted site, but if you watch the screen carefully, you'll notice that it's actually coming from a window underneath, what we call a pop-under window that's just lying in wait, hoping that this can happen in which case the user might think this download is for the trusted site and might click yes.

This next one which is one of my favorites is cancel means yes. If you look at this screen, it looks like an official security update or some kind of privacy update. In fact, if you read it carefully, it

says this is a security update, a personal privacy protection update and a system update. They've used every buzz word they can imagine and it's provided these okay and cancel buttons and it looks quite bona fide. The reality is is that this is actually just an image and none of these buttons are functional. In fact, if you click on the okay or even the little X in the corner, it will all take you to the site and attempt to download software to your machine. This is quite deceptive.

Here's another example of the same kind of trick. The security alert in this window is embedded and again provides the Yes/No cancel buttons, but it's just a picture and people can embed pictures in web pages. This is a normal thing. But it tricks users and they click somewhere on this window and one of these buttons and it still takes them to the site and attempts to download the software.

Another thing that bothers me about it is it says "warning, your computer is being attacked by spyware and adware." Well, how do they know that? I mean this is basically just scare tactics in order to get people to download this software.

Finally, in the browser there's a security setting. This is one other way that unwanted software can end up on your machine. If you set it to the low setting, it means that all sites you visit are trusted. I call this leaving your front door open. In this case, there's no warning, the software will simply load because you've told the system everything is trusted. We first off have a default which is medium and we recommend to users to leave it at medium or higher. So these slides provide just a sample of the ways users can be tricked. I've included other examples in my written testimony.

There is no silver bullet to address the wide range of issues with deceptive software. We believe it will take a comprehensive approach that has four key elements. The first is better consumer education. Today's hearing and last week's FTC workshop heightened consumer awareness of the problems caused by deceptive software. To complement these efforts, Microsoft recently launched a website www.microsoft.com/spyware to help consumers understand, identify, prevent and remove deceptive software.

The next element is technology. Microsoft will make available this summer a free update to Windows XP called Service Pack 2. It will include a new pop up blocker and pop ups is one of the most common ways that people get a proposition for a download through a pop up experience. Pop up blocker shows up in this thing called an information bar in Internet Explorer. It gives people both notice and choice of what's happening to them with the pop ups. They can choose to block them or choose to allow them through or do that by site.

I know my financial institution needs pop ups to work, so I would turn up pop ups for that site.

Another feature is this new download blocker. It specifically is designed to prevent forced downloads. These are downloads that are unsolicited. You go visit a website and somebody attempts to jam software on your machine. Instead of that happening, you get a little warning in this little information bar that says hey, someone is trying to download some software, what do you want to do? And you don't have to take any action. By having this blocker, you

don't have to be interrupted and take action and it's suppressed until you decide on your terms to do something about.

This helps with two problems. One is that it prevents the pop-under exploit I mentioned earlier and second, I have small kids and they don't even read and I ended up with some kind of spyware in my system because they clicked yes to some dialog that popped up in the middle of a game. This would prevent that from happening. They won't even see that opportunity to download this kind of software.

We've also cleaned up the install prompts. The one on the left is the old one and there's opportunity for some publishers to throw a lot more information there we had wanted originally which makes a very confusing experience. If you've actually looked at the one on the left more carefully, it's almost a miniature license agreement thrown in this experience which is totally inappropriate.

The one on the right makes that much more difficult to do and it truncates the line, makes it much easier to spot someone trying to trick you. We also added a new feature called never accept software from a publisher. So you could choose by publisher to say look, I don't want software from you anymore and block that from happening.

The last thing, as I mentioned earlier about leaving your front door open, it seems intuitively obvious well look, if low is kind of dangerous for most users, why do you offer it? So now we actually pop an arrow that says look, you really can't set it to low anymore. Expert users can get around this and if they want to lower their settings they can, but for the majority of users, at least we've done something to slow down this accidental way that they leave their doors open.

So these improvements, as well as others we are working on, will advance our goal of helping users better understand what software they are running and installing and whether they can trust it.

The third element of our approach is industry-wide best practices which we believe will create an incentive for legitimate software publishers to do the right thing. Best practices will also serve as a foundation for programs that certify good actors and thereby enable consumers to make more informed decisions. In the end, we believe self-regulatory measures will best account for the complexities of different software applications and evolve to meet the ever-changing nature of technology.

The fourth element is aggressive enforcement of existing laws. Such enforcement could put some of the most insidious violators out of business which would have a significant impact on the amount and the type of deceptive software that is produced and distributed in the United States.

Finally, for what is not already illegal under existing law, Federal legislation can help fill in the gaps. That said, any legislation must carefully target deceptive behavior rather than specific features or functionalities. My written testimony provides examples of areas in which legislation can impose ineffective or impractical requirements. As you consider legislating in this area, we urge you to avoid such unintended consequences.

In conclusion, we applaud the subcommittee for holding this hearing today and appreciate the opportunity to share our experi-

ence and recommendations. We are committed to working with you to thwart the efforts of those who produce industry-deceptive software and to restore choice and control to our customers.

Thank you.

[The prepared statement of Jeffrey Friedberg follows:]

PREPARED STATEMENT OF JEFFREY FRIEDBERG, DIRECTOR OF WINDOWS PRIVACY, MICROSOFT CORPORATION

Chairman Stearns, Ranking Member Schakowsky, and Members of the Subcommittee: My name is Jeffrey Friedberg, and I am the Director of Windows Privacy at Microsoft Corporation. I want to thank you for the opportunity to share with the Subcommittee our views on this burgeoning threat to computer users around the world. Spyware and other deceptive software share a common theme: they use ambiguity, coercion, deceit, and outright trickery to lure or even force users to execute or install unwanted and often invasive programs. Our customers complain that this software degrades their computing experiences—in some cases rendering their computers unusable—and causes them to feel frustrated and out of control. It also compromises their privacy and can make their computers more susceptible to attack.

Microsoft applauds Congress and the members of this Subcommittee for their attention to this problem. In particular, we would like to acknowledge Representatives Mary Bono and Ed Towns for the time and energy they have invested. Stopping the spread of deceptive software is one of Microsoft's highest priorities. We are committed to providing consumers with the information and technology that will help protect them against deceptive software. And we are committed to working with you, law enforcement, and others in the industry to identify and penalize the perpetrators of these nefarious programs.

Today, I want to describe the nature and nuances of deceptive software, and explain Microsoft's comprehensive strategy for tackling this issue. As with any issue that raises consumer protection concerns, there are a number of ways in which the public and private sectors, working together, can address the problem. These include educating consumers, developing new technology to help protect users and to empower them to make more informed choices, identifying industry standards and best practices, and taking enforcement actions against those engaged in fraudulent, deceptive, and unfair practices. To the degree existing law fails to capture bad actors, legislation could complement this strategy, but we believe it should be carefully crafted to target the bad behavior—not the underlying technology. Overbroad legislation could place an undue burden on legitimate software, and seriously undermine the user experience.

**What Is Deceptive Software?**

Let me explain what, exactly, I mean by *deceptive software.* Deceptive software generally describes programs that gain *unauthorized* access to a computer—whether to spy on user activities, hijack user configurations, or deliver intrusive and unwanted pop-up advertisements. The common thread that unifies deceptive software programs—and that distinguishes them from legitimate applications—is their lack of notice and choice, and their absence of respect for users' ability to control their own computers. With proper disclosure, user authorization and control, these same features can be an asset: user-approved tracking can lead to personalization; user-approved configuration changes (for example, setting a new search page) can yield a better user experience; and user-approved displaying of advertisements can subsidize the cost of a service (such as e-mail), making it cheaper or even free for consumers. In short, the problem is with bad practices, not the underlying features.

There is a spectrum of tricks that cause consumers to load software applications that they may not want. To better understand these tricks, it is useful to first briefly describe a legitimate download experience. I would like to draw your attention to Slide A: "User Initiates Download." This slide represents a typical web site consumers might visit. On the web site is a link for downloading a program (in this example, a program that will display a "stock ticker"). When users click on the link, the operating system displays a security warning that asks them whether they want to install the program, as shown in Slide B: "Security Warning Displayed." These security warnings are a normal part of the computing experience.

In some instances, however, web sites manipulate the download experience in an attempt to mislead users. When users are presented with a download request and security warning, they will often consider the web site they are visiting to decide whether to accept the download. If the web site is one they trust, they may simply accept the download without much thought. Using a deceptive technique we call a

*pop-under exploit,* however, some web sites take advantage of this trust, going out of their way to make it more difficult for users to tell which web site is actually offering the download. For example, on Slide C: "Pop-Under Exploit—Step 1," users who are visiting a legitimate website are presented with a download request that appears to have been generated from that site, which we see on Slide D: "Pop-Under Exploit—Step 2." In fact, the download request was actually launched from a web page that is hidden beneath the legitimate site, as we see on Slide E: "Pop-Under Exploit—The Trick." Launching a download request from a pop-under can result in a confusing or even misleading experience. It is likely that the user, who cannot easily view the underlying web page, will assume that the request came from the legitimate site and may choose to download the software for this reason.

Web sites are often compensated for each software download that occurs from their site and in order to increase this volume, some web sites will resort to deceptive practices. For example, a web site might confuse users so that no matter where they click, they are taken to a page that requires a download. In this scenario, shown on Slide F: "'Cancel' Means 'Yes,'" a user is presented with an image that mimics a security warning or update and appears to provide the user with appropriate choices about downloading certain software. However, even if the user clicks the "Cancel" button or the "[x]" box to close the window, the web site will attempt to download the software onto the user's machine. This type of trick can also take place through embedded security alerts, as shown on Slide G: "Faux Security Alert," where all buttons in the alert mean "yes" and initiate a download experience the user did not want.

Perhaps the most nefarious way that software is installed requires no action on the part of the user. In this scenario, bad actors exploit a security hole and covertly install software without any notice to or consent from the user. This practice is illegal under existing law, but bad actors still attempt to deceive users in this fashion. To educate consumers on the steps they can take to minimize this risk, we created a web site, www.microsoft.com/protect, that recommends (1) keeping systems up to date using the free Windows Update service, (2) running up-to-date anti-virus software, and (3) using a firewall like the one included with Windows XP.

There is one other way that software can get installed without any action on the part of the user. If a user sets their browser security setting to "low," as illustrated on Slide H: "Don't Leave Your Front Door Open," all sites are assumed to be "trusted," and no security warning will be displayed. This can result in what are called "drive-by-downloads," in which the download silently and automatically occurs by just visiting a web site. Microsoft encourages users to leave their security settings on the default setting of "medium" or higher, and in cases where the browser security level must be set on "low," we encourage users to reset security back to a higher level as soon as possible.

These slides illustrate just a few of the ways in which users can be tricked into downloading unwanted and sometimes destructive software. Other tricks include limiting users' ability to make a fair choice by repeatedly asking them to make a decision until they say "yes"; covertly installing software by piggybacking on other software being installed; pretending to uninstall; and re-installing without authorization.

**Deceptive Software is a Growing Problem for Our Customers**

Our customers are becoming increasingly frustrated by unwanted and deceptive software. We receive thousands of calls from customers each month directly related to unwanted or deceptive software, and we have evidence that suggests such software is at least partially responsible for approximately one-half of all application crashes that our customers report to us. In addition, our industry partners who make computers—sometimes referred to as "Original Equipment Manufacturers" or OEMs—have indicated that unwanted and deceptive software is one of the top support issues they face, and that it costs many of the larger OEMs millions of dollars per year.

Other estimates support the growing threat of the problem. According to the security software firm PC Pitstop, nearly a quarter of personal computers are afflicted with some type of unwanted or deceptive software application. More aggressive estimates place the total at between 80 and 90 percent of all PCs. Indeed, a 2003 study by the National Cyber Alliance found that 91 percent of broadband customers have some form of unwanted or deceptive software on their home computers.

What may be most alarming is the growth of these programs over the past year. PestPatrol, which sells spyware detection and removal software, estimates that there are now more than 78,000 separate spyware programs in use. In the past year, PestPatrol identified more than 500 new Trojan horses (which are programs that provide unlimited access to PCs), 500 new key loggers (which monitor and

record a user's keystrokes), and nearly 1,300 new forms of programs that display advertisements. The past year has also seen spyware manufacturers gain strides in their ongoing technological battle against anti-spyware removal and detection systems. Over the past six months, the number of "burrowers"—programs that dig so deeply into an operating system that they cannot be found or removed without major and potentially damaging surgery—has increased from six to more than 40.

The explosion in the volume of unwanted and deceptive software has had an enormous impact on Microsoft, as has the accompanying increase in the complexity with which those programs operate and the damage that they do. Many of our customers blame the problems caused by these programs on Microsoft software, believing that their systems are operating slowly, improperly, or not at all because of flaws in our products or other legitimate software. This costs us not only millions of dollars per year in otherwise unnecessary support calls, but also immeasurable damage to our reputation and, most importantly, to our efforts to optimize our customers' computer experiences.

**Adopting a Comprehensive Strategy To Combat Unwanted and Deceptive Software**

As I have shown, there is a continuum of behaviors that lead or trick users into downloading unwanted software programs. In the same vein, there is a continuum of solutions that we believe must be part of the strategy to end these behaviors and curb the spread of deceptive software. This strategy has four prongs: widespread customer education; innovative technology solutions; improved industry self-regulation; and aggressive enforcement under existing state and federal laws. As I mentioned previously, new, carefully crafted and narrowly focused legislation can also play a role to the extent that existing laws do not fully address certain deceptive or misleading practices.

*Addressing the Problem Starts with Consumer Education*

The first step in the battle against unwanted and deceptive software is better consumer education. Once confined to the back pages of industry journals, the problem is beginning to move to the mainstream of consumer protection issues, as last week's workshop at the Federal Trade Commission and today's hearing demonstrate. These public forums are essential in heightening consumer awareness of the problems caused by deceptive software.

To complement those efforts, Microsoft recently launched a website—www.microsoft.com/spyware—with information that is specifically designed to help consumers understand, identify, prevent, and remove unwanted and deceptive software. This website explains what spyware is and why it can be dangerous; tells users how they can protect their machines from being compromised by these unauthorized programs; helps consumers ascertain whether their computers already contain unwanted or deceptive software by describing its symptoms, such as sluggish performance, an increase in random pop-up advertisements, and a hijacked home page; and points users to third-party tools that can detect and remove these programs.

Microsoft is committed to working with Congress and the FTC to continue educating consumers about the ways they can prevent unwanted and deceptive software from attacking their PCs. While the Internet is an incredible resource that has enabled—and will continue to enable—countless and sweeping improvements in communications, commerce, and government, that same power requires that computer users take the same care for their safety and security online as they would offline. As an industry leader, we acknowledge and strive to fulfill our responsibility to educate consumers about these and other related issues. Consumers who take steps to remove or prevent the installation of this software will not only preserve their own privacy, security, and optimum computer experiences, but they will make an important contribution to the larger effort of generally eliminating the problem. The entities that produce these programs will have much less incentive to create and download their products if consumers take steps to block their use—or at least do not respond to the seller on whose behalf the deceptive software purveyor is operating.

*Industry Is Working on New Technology To Combat Deceptive Software*

The development of anti-spyware technology should complement the impact of consumer education and awareness. For example, third parties have released anti-spyware programs that enable users to remove or disable many examples of unwanted and deceptive software from their PCs without damaging their existing hardware or legitimate software. These tools are continually being improved to address new variants and scenarios.

Microsoft is working on enhancements that will also help address the problem. For example, we will soon be introducing Windows XP Service Pack 2—a free update for all licensed Windows XP users—that includes features designed to block some of the entry points and distribution methods of deceptive software by better informing users in advance about the type of software they will be installing. These enhancements include:

- A new pop-up blocker, turned on by default, that will reduce a user's exposure to unsolicited downloads (*See* Slide I: "New Popup Blocker");
- A new download blocker that will suppress unsolicited downloads until the user expresses interest (*See* Slide J: "New Download Blocker");
- Redesigned security warnings that make it easier for users to understand what software is to be downloaded, make it more obvious when bad practices are used (e.g., multi-line program names), and allow users to choose to never install certain types of software (*See* Slide K: "Improved Install Prompts");
- A new policy that restricts a user's ability to directly select "low" security settings (*See* Slide L: "Harder to Leave Your Front Door Open"); and,
- Tools to help expert users and support professionals understand and disable unwanted functionalities that have been added to the browser. (*See* Slide M: "New Add-On Manager.")

Beyond Windows XP Service Pack 2, Microsoft is investing in future technologies that advance our goal of giving users the ability to understand what software they are running and installing, and whether they can trust it. We continue to explore ways that we can better inform consumers in advance about programs that they plan to install, and to provide them with more control over the installation itself. We also are striving to enhance and simplify the ways in which our customers can see what software is running on their computers, and to evaluate what to do with that software based on their preferences. And we are working to advance technologies that can be used by our entire spectrum of customers—from the most sophisticated enterprise to the most novice consumer—because we want them all to have an equally fulfilling computer experience.

*Industry Best Practices Are an Important Part of the Solution*

The third important part of our strategy is to develop a set of industry-wide best practices. Developing best practices is critical because they will create an incentive for legitimate software publishers to distinguish themselves from less scrupulous publishers and minimize the risk of being classified with the bad actors that engage in deceptive practices. Best practices will also serve as a foundation for programs that certify and label good actors and thereby enable users to make more informed decisions about the type of software they execute and install on their computers.

The first step in this process is developing an understanding of the devious, deceptive, or unfair practices that adversely affect consumers. The Center for Democracy and Technology (CDT) has made great strides in this area through its Consumer Software Working Group, of which we are a member. This group includes public interest organizations, software companies, Internet service providers, and hardware manufacturers, all of whom have worked hard to identify a set of deceptive practices that raise serious concerns. These practices—many (if not all) of which are illegal under existing law—should help focus regulatory and law enforcement efforts on the truly bad actors.

In addition to recognizing bad practices, we think it is equally important to begin to develop best practices in certain scenarios. These scenarios include the collection and transmission of personal information, the display of advertisements, and changes to configuration settings that affect the Internet browser home page or browser search page. The touchstone of these best practices should be appropriate notice and consent. Users should understand what the software will do in these scenarios before it is executed, and they should then have a choice about whether to execute it. In addition, programs with these features that are installed on a user's computer should also be easily uninstalled or disabled—or if that is not possible, the user should be clearly informed of that fact upfront.

Microsoft is actively extending its best practices to explicitly include the scenarios highlighted above. We are committed to working with other companies in the industry to ensure that users have high-quality experiences with legitimate software. And we would be happy to share our best practices to the extent they would be helpful in moving the industry forward to this common goal. In the end, self-regulatory measures more than federal requirements will help industry leaders define and implement best practices that account for the complexities of different software applications and can evolve to meet the ever-changing nature of technology.

*Enforcement Is a Critical Part of the Fight Against Deceptive Software*

A fourth key weapon to stop the spread of deceptive software is the aggressive enforcement of existing laws. Such enforcement could put some of the most insidious violators out of business, which would have a significant impact on the amount and type of deceptive software that is produced and distributed in the United States. Moreover, a few targeted enforcement actions would serve as a powerful deterrent to other manufacturers of deceptive software.

Enforcement actions are possible using existing law. For example, under the Federal Trade Commission Act, the FTC is empowered to challenge unfair and deceptive trade practices, which—by definition—are at the heart of virtually all deceptive software programs. Many states have similar laws that authorize their own enforcement agencies to prosecute entities that engage in these same types of practices. And the Computer Fraud and Abuse Act provides other law enforcement agencies with the means to address spyware threats that involve hacking into users' computers. Given the growing sophistication, diversity, and proliferation of spyware, the private and public sectors should combine their resources to hold those who publish illegitimate deceptive software accountable for their actions and the damage they perpetrate.

**Congress Should Proceed Cautiously**

Microsoft is hopeful that the combination of user education, improved technology, industry best practices, and enforcement of existing laws can effectively combat the growing problem of deceptive software. Although we have seen an increase in the amount and complexity of deceptive software in recent months, it is encouraging to see the stepped-up response of both the public and private sectors. We are open to considering whether federal legislation can provide an additional layer of protection and another weapon in the fight against deceptive software. However, Microsoft offers two important caveats when considering federal legislation.

*First,* as noted above, many deceptive software programs are already either prohibited under existing law—such as the Computer Fraud and Abuse Act—or are subject to the FTC's jurisdiction over unfair and deceptive trade practices. Any additional federal legislation deemed necessary to outlaw deceptive software must be carefully crafted to supplement the existing legal framework only where gaps are identified.

*Second,* any legislation should target deceptive behavior, rather than specific features or functionalities, to avoid imposing unworkable requirements on legitimate programs and negatively impacting computer users. Examples of some unintended consequences of well-intentioned legislation include the following:

- *Disruptive User Experience.* Many legitimate software programs contain an information-gathering activity to perform properly, including error reporting applications, troubleshooting and maintenance programs, security protocols, and Internet browsers. Imposing notice and consent requirements every time these legitimate programs collect and transmit a piece of information would disrupt the computing experience, because users would be flooded with constant, non-bypassable warnings—making it impossible to perform routine Internet functions (such as connecting to a web page) without intolerable delay and distraction.
- *Compromised Consent Experience.* "One size fits all" notice and consent requirements may not give users sufficient context to make informed decisions. For example, requiring notice and consent at the time of installation ignores the importance of a technique we refer to as "just in time" consent, which delays the notice and consent experience until the time most relevant to the user—just before the feature is executed. If a program crashes, for instance, Windows Error Reporting functionality will ask the user whether he or she would like to send crash information to Microsoft. At this time, the user is able to examine the type of information that will be sent to Microsoft and to assess the actual privacy impact, if any, of transmitting such information in light of the potential benefit of receiving a possible fix for the problem. In this case, the user understands the costs and benefits of the proposition being made and is able to make an informed choice. Presenting the notice and choice experience at the time of installation, on the other hand, would lack this critical context.
- *Unrealistic Uninstall Requirements.* Requiring standardized uninstall practices for all software would be unworkable in many circumstances. For example, there are cases where a full and complete uninstall is neither technically possible nor desirable, such as with a software component that is in use and shared by other programs. In addition, there are other cases where an uninstall may be technically possible, but the cost to provide such functionality would be prohibitive, such as with complex software systems that may require the entire software

system to be removed. Finally, there are situations where requiring uninstall could actually comprise the security of the system, such as backing out security upgrades or removing critical services.

There are many other areas in which legislation could fall into similar traps, imposing ineffective or impracticable requirements, or even threatening PC security and usability. We therefore encourage Congress to focus its attention on the devious practices of deceptive software, including those identified by CDT and its Consumer Software Working Group; to legislate only to the extent such practices are not already illegal under existing law; and to engage industry experts in understanding the complexities of software, thereby ensuring appropriate due diligence to avoid unintended consequences.

Unwanted and deceptive software is a growing problem, and we believe that a multi-faceted approach is needed: improved consumer education; new technology solutions; a comprehensive set of industry best practices; and aggressive enforcement of existing laws against violators. This approach will enable consumers to make more informed decisions about installing software; help distinguish good actors from bad ones; and make being bad an expensive proposition. We commend the Subcommittee for holding this hearing today and thank you for extending us an invitation to share our experience and recommendations with you. Microsoft is committed to working with you to thwart the efforts of those who produce and distribute these deceptive programs, and to restoring choice and control back where it belongs—in the hands of consumers.

# Statement of Jeffrey Friedberg,
## Director of Windows Privacy,
## Microsoft Corporation

Testimony Before the House Committee on Energy and Commerce
Subcommittee on Commerce, Trade, and Consumer Protection

**"Spyware: What You Don't Know Can Hurt You"**

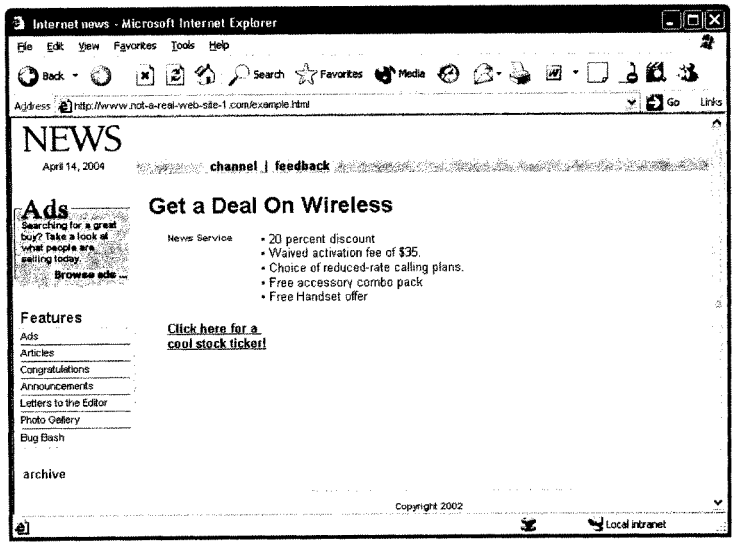
*Slides*

*The example companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, places, or events is intended or should be inferred.*

# Normal Download Experience

*Slide A*

# User Initiates Download

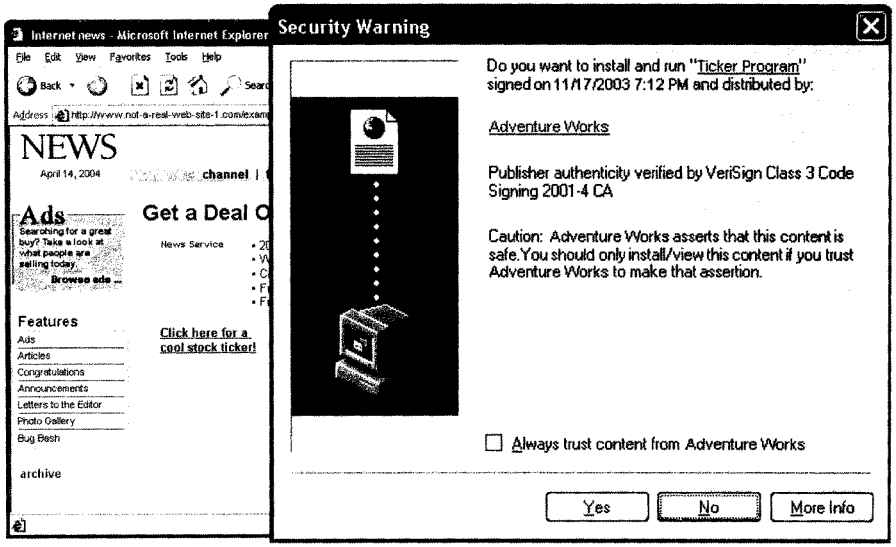



April 29, 2004 Microsoft Corporation 3

•User visits a web site, sees some software they want, and clicks on the link.

*Slide B*

# Security Warning Displayed




April 29, 2004 Microsoft Corporation 4

- User will get Security warning when downloading programs.
- User makes a choice whether to install.

# Some Common Tricks

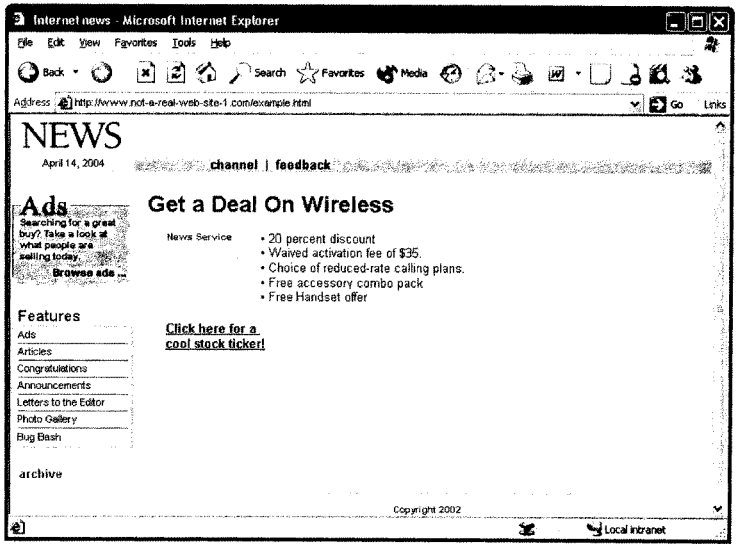


•Some common tricks that may lead a user to install software they do not want.

# Pop-Under Exploit

***Slide C***

## Step 1: User visits a trusted web site



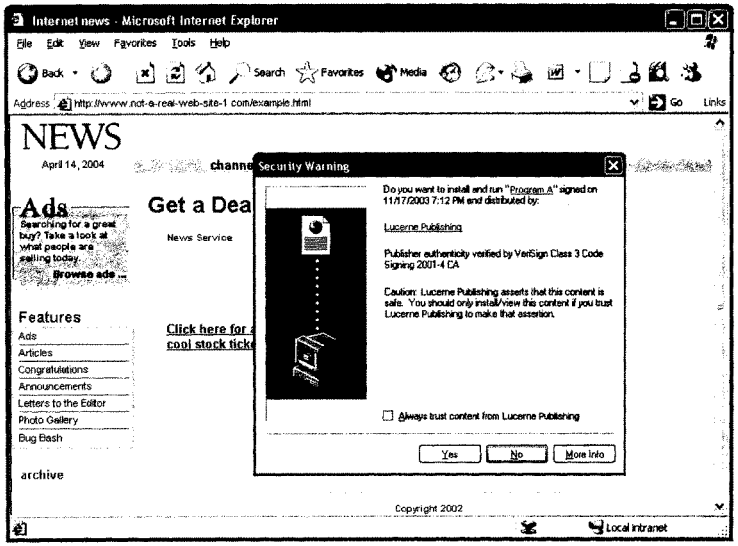

April 29, 2004 Microsoft Corporation 6

•User visits a web site they trust.

# Pop-Under Exploit

***Slide D***

## Step 2: After a delay, user gets offer to install a program




April 29, 2004 Microsoft Corporation 7

- User gets offer to download a program.
- They think the download offer is from the web site they trust, but …

# Pop-Under Exploit

**Slide E**

## The Trick: download is really from a hidden window!

Moving top window out of the way will expose hidden window

Hidden Window

Sample Pop-Under - Microsoft Internet Explorer

**This pop-under window embeds an ActiveX control which will be presented to the user above whatever page is on top.**

Security Warning

Do you want to install and run "Program A" signed on 11/17/2003 7:12 PM and distributed by:

Lucerne Publishing

Publisher authenticity verified by VeriSign Class 3 Code Signing 2001-4 CA

Caution: Lucerne Publishing asserts that this content is safe. You should only install/view this content if you trust Lucerne Publishing to make that assertion.

Always trust content from Lucerne Publishing

Yes | No | More Info

Internet news - Microsoft Internet Exp

File Edit View Favorites Tools Help

Back

Address http://www.not-a-real-web-site-1.com/

Go Links

NEWS

April 14, 2004

Ads

Searching for a great buy? Take a look at what people are selling today.

Browse ads ...

Get a Dea

News Service

Features

Ads

Articles

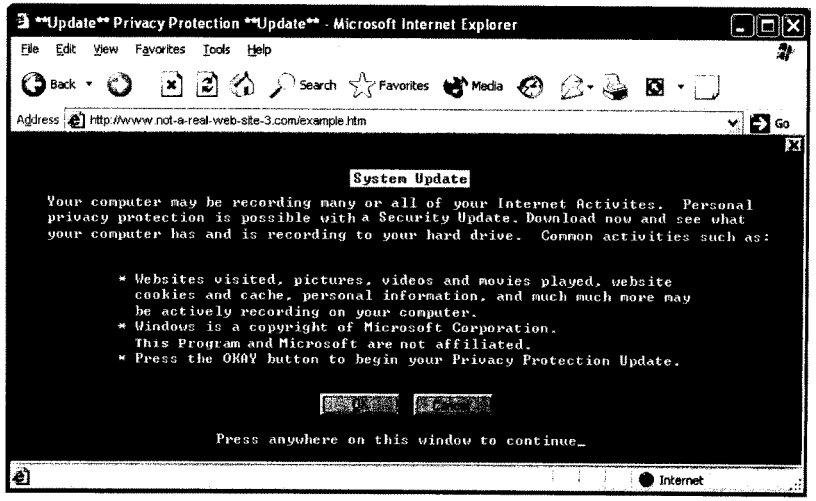
Click here for a cool stock ticker!



- Download offer is really from a hidden "pop-under" window.
- To user it's unclear which page is offering the download. May assume it's for the trusted page.

*Slide F*

# "Cancel" Means "Yes"



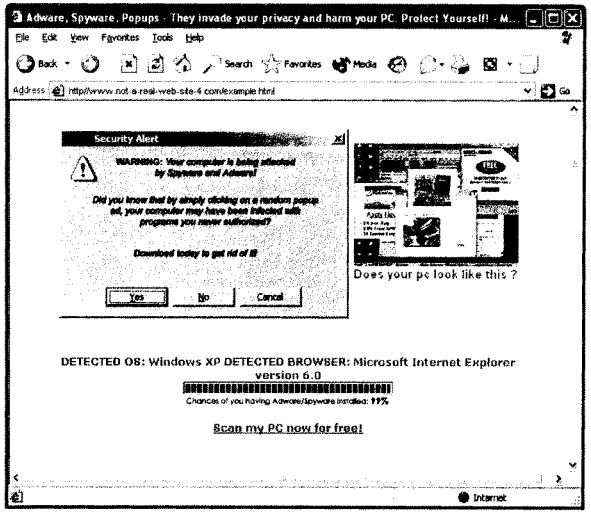

April 29, 2004 Microsoft Corporation 9

- The "Cancel" button and even the [x] in the corner all mean "OK". In fact, the buttons and text are really just a "picture" and not functional.
- The window also tries to impersonate an official System/Security Update.

*Slide G*

# Faux Security Alert

(really just a picture)

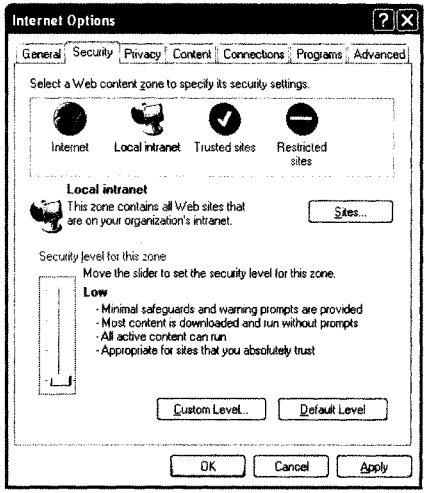





- Same as previous example, but this one is an embedded security alert. All buttons mean "yes".
- Also, the alert asserts "Your computer is being attacked" which may not be the case.

*Slide H*

# Don't Leave Your Front Door Open




April 29, 2004 Microsoft Corporation 11

- Setting on low allows silent "drive by" downloads. No security warning will be displayed ("low" means you trust the sites you visit).
- Should leave on Medium or better (default is Medium). If must set to low, reset ASAP when done.

# Some XP SP2 Enhancements that Help Address the Problem

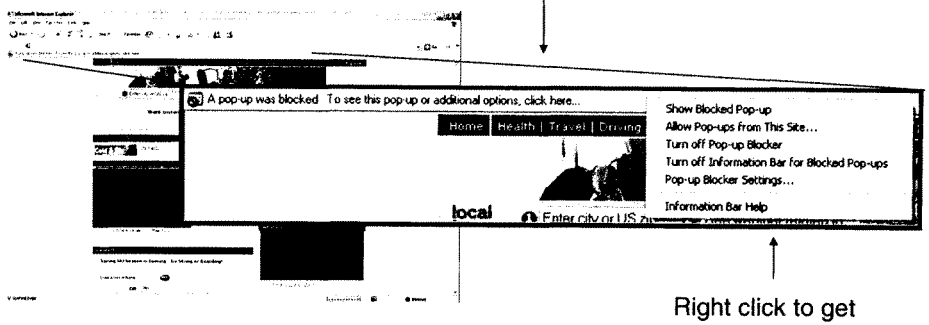


•These are planned for Windows XP Service Pack 2.

*Slide I*

# New Popup Blocker

Information Bar provides
Notice and Choice



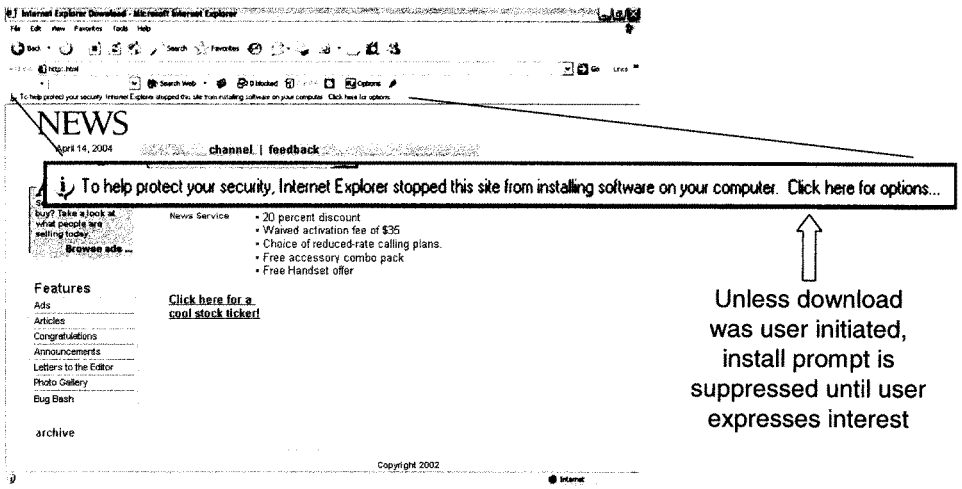

Right click to get
more options

April 29, 2004 Microsoft Corporation 13

- Pop-up Blocker empowers users with control over a disruptive experience.
- Fewer pop-ups means fewer opportunities to download unwanted software.

*Slide J*

# New Download Blocker



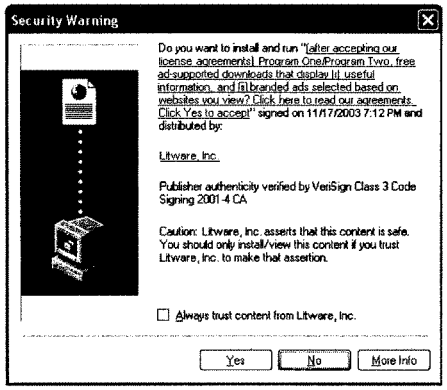

Unless download was user initiated, install prompt is suppressed until user expresses interest

April 29, 2004 Microsoft Corporation 14

- Suppresses unsolicited program downloads until user expresses interest.
- Prevents pop-under exploit (program download is tied to page that offered it).

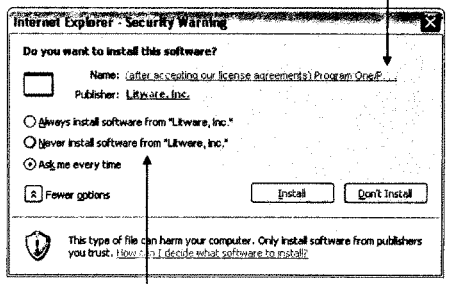
***Slide K***

# Improved Install Prompts




***Current***

Cannot overload text fields




***New***

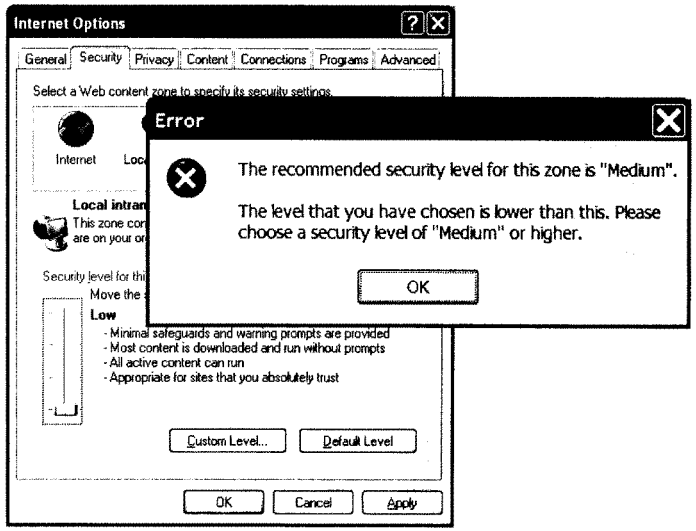
Can choose "Never Install"



- Cleaner presentation that is less confusing.
- Can choose "Never Install" software from a particular publisher.

*Slide L*

# Harder to Leave Your Front Door Open

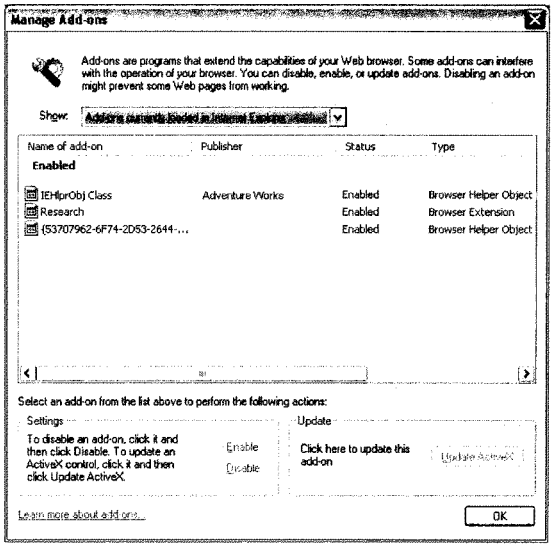



April 29, 2004 Microsoft Corporation 16

- Can no longer directly set the security slider to "Low."
- Expert users can still use advanced options to reduce security if they want to.

*Slide M*

# New Add-on Manager




User can Enable/Disable ActiveX Controls and Browser Helper Objects (e.g. Toolbars)

Neutralize unwanted software



- View and disable unwanted browser add-ons such as toolbars.
- Helps expert users and support professionals diagnose problems and provide quick relief.

Mr. STEARNS. I thank you for your demonstration.

Mr. David Baker, who is Vice President, Law and Public Policy with Earthlink. We welcome you.

**STATEMENT OF DAVID N. BAKER**

Mr. BAKER. Mr. Chairman Stearns, Ranking Member Schakowsky, ladies and gentlemen of the committee, thank you for inviting me here today. I'm Dave Baker, Vice President for Law and Public Policy with Earthlink, headquartered in Atlanta. Earthlink is the Nation's third largest internet service provider, serving over 5 million customers nationwide with dial-up, broadband, web posting and wireless internet services.

Earthlink is always striking to improve its customers online experience. To that end, we appreciate the attention this committee is paying to the growing problem of spyware. We may be at the point in time with regard to the development and proliferation of spyware that we were just a year or 2 ago with spam. In other words, spyware is just now being noticed by many consumers, yet threatens to grow to the point where it could soon compromise their online experience and security if it does not do so already.

As the Wall Street Journal noted just this past Monday, April 26, "indeed spyware, small programs that install themselves on computers to serve up advertising, monitor web surfing and other computer activities and carry out other orders is quickly replacing spam as the online annoyance computer users most complain about."

Also like spam, we must fight spyware on several fronts, using legislation, enforcement, customer education and technology solutions. To this end, we applaud the efforts of Congresswoman Bono, Congressman Towns, other members and this committee to introduce legislation such as H.R. 2929, the Safeguard Against Privacy Invasions or SPI Act, prohibiting the installation of software without consent, requiring uninstall capability, establishing requirements for transmission pursuant to license agreements and requiring notices for collection of personally identifiable information, intent to advertise, and modification of user settings are all steps that will empower consumers and keep them in control of their computers and their online experience.

As a leading internet provider, EarthLink is on the front lines in combating spyware. EarthLink makes available to both its customers and the general public technology solutions to spyware such as EarthLink Spy Audit powered by Webroot. Spy Audit is a free service that allows users to quickly examine his or her computer and detect spyware. A free download of Spy Audit is available at our website and a screen shot of this web page is attached as Exhibit A to my testimony. EarthLink members also have access to Spyware Blocker which disabled all common forms of spyware including adware, system monitors, key loggers and Trojans. EarthLink Spyware Blocker is available free for EarthLink members as a part of Total Access 2004, our internet access software and a screen shot with information on Spyware Blocker is attached as Exhibit B to my testimony.

We include useful tools such as spamBlocker, Pop-Up Blocker, Virus Blocker, Privacy Tools and Parental Controls in addition to

Spyware Blocker and we will soon be introducing Scam Blocker which will help users detect and avoid nefarious fisher sites.

On April 15, 2004, EarthLink and Webroot announced the results of their Spyware Audit report. Over 1 million Spy Audit scans performed from January 1 through March 31st of this found over 29.5 million instances of spyware. This represents almost 28 instances of spyware per scanned PC. While approximately 23.8 million of these installations were mostly harmless adware cookies, the scans revealed over 5.3 million installations of adware and more seriously, over 184,000 system monitors, and almost 185,000 Trojans. A copy of the EarthLink/Webroot press release detailing these findings is attached as Exhibit C to my testimony.

Spyware is thus a growing problem that demands the attention of Congress, the FTC, consumers and industry alike. Through the efforts of Congress to introduce legislation like the SPI Act, the FTC to investigate the issue at its recent spyware workshop and through industry development of anti-ware tools, we can all help protect consumers against a threat that is often unseen, but very much real.

Thank you for having me here today.

[The prepared statement of David N. Baker follows:]

PREPARED STATEMENT OF DAVID N. BAKER, VP, LAW & PUBLIC POLICY, EARTHLINK, INC.

Mr. Chairman, Ladies and Gentlemen of the Committee, thank you for inviting me here today. I am Dave Baker, Vice President for Law and Public Policy with EarthLink. Headquartered in Atlanta, EarthLink is the nation's 3rd largest Internet Service Provider (ISP), serving over 5 million customers nationwide with dial-up, broadband (DSL, cable and satellite), web hosting and wireless Internet services. EarthLink is always striving to improve its customers' online experience. To that end, we appreciate the attention this committee is paying to the growing problem of spyware.

**Spyware: The Next Spam?**

We may be at a point in time with regard to the development and proliferation of spyware that we were just a year or two ago with spam. In other words, spyware is just now being noticed by many consumers yet threatens to grow to the point where it could soon compromise their online experience and security, if it does not do so already.

As the Wall Street Journal noted just this past Monday, April 26, "Indeed, spyware—small programs that install themselves on computers to serve up advertising, monitor Web surfing and other computer activities, and carry out other orders—is quickly replacing spam as the online annoyance computer users most complain about."

Also like spam, we must fight spyware on several fronts, using legislation, enforcement, customer education and technology solutions. To this end, we applaud the efforts of Congress and this committee to introduce legislation such as H.R. 2929, the Safeguard Against Privacy Invasions (SPI) Act. Prohibiting the installation of software without consent, requiring uninstall capability, establishing requirements for transmission pursuant to license agreements, and requiring notices for collection of personally identifiable information, intent to advertise and modification of user settings are all steps that will empower consumers and keep them in control of their computers and their online experience.

**EarthLink Experience**

As a leading Internet provider, EarthLink is on the front lines in combating spyware. EarthLink makes available to both its customers and the general public technology solutions to spyware such as EarthLink Spy Audit powered by Webroot ("Spy Audit"). Spy Audit is a free service that allows a user to quickly examine his or her computer and detect spyware. A free download of Spy Audit is available at www.earthlink.net/spyaudit. (See Exhibit A, attached hereto.) EarthLink members also have access to EarthLink Spyware Blocker, which disables all common forms

of spyware including adware, system monitors, key loggers and Trojans. EarthLink Spyware Blocker is available free for EarthLink members as part of Total Access 2004, our Internet access software. See www.earthlink.net/home/software/spyblocker (Exhibit B, attached hereto).

Total Access 2004 includes useful tools such as spamBlocker, Pop-Up Blocker, Virus Blocker, Privacy Tools and Parental Controls in addition to Spyware Blocker.

On April 15, 2004, EarthLink and Webroot announced the results of their Spy Audit report. Over 1 million Spy Audit scams performed from January 1, 2004 to March 31, 2004 found over 29,500,000 instances of spyware. This represents almost 28 instances of spyware per scanned PC. While approximately 23.8 million of these installations were mostly harmless adware cookies, the scans revealed over 5.3 million installations of adware, and more seriously, over 184,000 system monitors, and almost 185,000 Trojans. A copy of the EarthLink/Webroot press release detailing these findings is attached hereto as Exhibit C.

**Conclusion**

Spyware is thus a growing problem that demands the attention of Congress, the FTC, consumers and industry alike. Through the efforts of Congress to introduce legislation like the SPI Act, the FTC to investigate the issue at its recent spyware workshop, and through industry development of anti-spyware tools, we can all help protect consumers against a threat that is often unseen, but very much real.

Thank you for your time today.

Mr. STEARNS. I thank the gentleman. I'm going to go to the Honorable Mozelle Thompson, Commissioner, Federal Trade Commission and welcome you.

## STATEMENT OF HON. MOZELLE W. THOMPSON

Mr. THOMPSON. Thank you, Mr. Chairman and Ranking Member Schakowsky, members of the committee and subcommittee. It's good to see you.

As you know, I'm Commissioner at the FTC and I wish to thank the committee for holding this hearing on the important subject of spyware. I also appreciate the opportunity to appear before you today.

As you know—well, first, let me begin by telling you the views I express here are my own and not necessarily those of the Commission.

As you know, the FTC has long been involved with internet issues like online privacy, identity theft, cross border fraud and spam. And our experience has given us a unique vantage point to view developments in the consumer marketplace and identify issues that warrant public attention.

Last week, the Commission held a 1-day public workshop on one of those topics, the distribution and effects of software commonly referred to as spyware. We began our workshop by asking participants to define what spyware is. As the chairman noted, spyware commonly refers to software that essentially monitors consumers' computing habits and as such, it necessarily raises privacy issues. This software can offer consumers and businesses various benefits, including a streamline interactive online experience and updates and can allow businesses to more effectively communicate with their customers. However, spyware can also be used as secret software that surreptitiously gathers information and transmits it to third parties without the subject's knowledge or consent. Sometimes these uses can result in identity theft and other types of fraud and in some cases can interfere with the computer's operability.

These activities undermine consumer confidence in the marketplace and can also impose extra costs on good actors who are forced to compete against those willing to engage in deception, fraud or worse.

I used our workshop as an opportunity to challenge industry to promptly develop a set of best practices with respect to spyware. These practices should contain several critical elements including meaningful notice and choice so the consumers can make informed decisions about whether or not they wish to deal with an online business that uses monitoring spyware or partners with companies that do.

I also asked industry to develop a public campaign to educate consumers and businesses about what spyware is and how it operates. This public campaign should also discuss the array of technological tools that are available for consumer use. Finally, I called upon industry to establish a mechanism that will allow businesses and consumers to maintain a continuing dialog on how government can take action against those who do wrong and undermine consumer confidence through the misuse of spyware.

Now some Members of Congress, including Representative Bono and Towns, are calling for spyware legislation. I commend you for bringing important public attention to this issue. And I understand the desire to take action before the problems associated with spyware grow worse and injure more consumers and businesses, but I do not believe legislation is the answer at this time.

Instead, I respectfully submit that we should give industry an opportunity to respond to my challenge. My experience working on issues like online privacy and spam tells me that in approaching such problems any solution must at the very least be based on transparency, adequate notice and consumer choice. So I've used my challenge as a way to set out what I consider to be the critical elements that should form a baseline for any industry response. If the self-regulatory response is not timely or is inadequate, another perhaps legislative approach might be appropriate.

In any event, whatever is done in this area should work in conjunction with existing laws like the FTC Act which allows the Commission to take action against deceptive or unfair practices.

I make this suggestion with some circumspection, recognizing that there are many who would like Congress to act now. But absent a comprehensive data privacy law in the United States and recognizing the challenge posed by defining spyware because it has beneficial and not beneficial uses, I believe that self-regulation, combined with enforcement of existing laws will help address many of the issues raised in this area.

I am also aware that States might be anxious to legislate here, but I ask them to be cautious as well because a patchwork of differing and inconsistent State approaches might be confusing to industry and consumers alike.

Now finally, as I mentioned, spyware raises important privacy concerns and several years ago I appeared before Congress and suggested that a Federal law incorporating fair information practices might be an acceptable legislative response. I believe it may still be, but I don't think it will be the most effective in addressing the problems posed by spyware.

For the time being, however, a strong, responsible and prompt industry self-regulatory response may provide an effective solution for the problems that spyware poses for both consumers and industry.

Thank you very much.

[The prepared statement of Hon. Mozelle W. Thompson follows:]

PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION

Mr. Chairman and members of the Committee, the Federal Trade Commission ("Commission" or "FTC") appreciates this opportunity to provide the Commission's views on "spyware." [1]

The FTC has a broad mandate to prevent unfair competition and unfair or deceptive acts or practices in the marketplace. Section 5 of the Federal Trade Commission Act gives the agency the authority to challenge acts and practices in or affecting commerce that are unfair or deceptive.[2] The Commission's law enforcement activities against unfair or deceptive acts and practices are generally designed to promote informed consumer choice. This statement will discuss the FTC's activities related to spyware, including our recent workshop and potential law enforcement actions.

FTC SPYWARE WORKSHOP

For nearly a decade, the FTC has addressed online privacy and security issues affecting consumers. Through a series of workshops and hearings, the Commission has sought to understand the online marketplace and its information practices, to assess the impact of these practices on consumers, and to challenge industry leaders to develop and implement meaningful self-regulatory programs.[3]

The most recent example of this approach is the workshop entitled "Monitoring Software on Your PC: Spyware, Adware, and Other Software" that was held last week. The workshop was designed to provide us with information about the nature and extent of problems related to spyware, and possible responses to those problems. Specifically, the workshop focused on four main topics: (1) defining "spyware" and exploring how it is distributed (including the role of peer-to-peer file-sharing software and whether spyware may differ from "adware"); (2) examining spyware's general effects on consumers and competition; (3) exploring spyware's potential security and privacy risks; and (4) identifying technological solutions, industry initiatives, and governmental responses (including consumer education) related to spyware. Underscoring the importance of this issue both FTC Commissioners Orson Swindle and Mozelle Thompson personally participated in the workshop.

To encourage broad-based participation, the FTC issued a Federal Register Notice announcing the workshop and requesting public comment.[4] The Commission received approximately 200 comments, and the record will remain open until May 21, 2004, for submission of additional comments. At the workshop, a wide range of panelists engaged in a spirited debate concerning spyware, including what government, industry, and consumers ought to do to respond to the risks associated with spyware.

Although the agency is continuing to receive information on this important issue, the record at the workshop leads to some preliminary conclusions. First, perhaps the most challenging task is to carefully and clearly define the issue. "Spyware" is an elastic and vague term that has been used to describe a wide range of software.[5] Some definitions of spyware could be so broad that they cover software that is beneficial or benign; software that is beneficial but misused; or software that is just poorly written or has inefficient code. Indeed, there continues to be considerable debate regarding whether "adware" should be considered spyware. Given the risks of

[1] The written statement presents the views of the Federal Trade Commission. Oral statements and responses to questions reflect the views of the speaker and do not necessarily reflect the views of the Commission or any other Commissioner.

[2] 15 U.S.C. § 45.

[3] See, e.g., Workshop: Technologies for Protecting Personal Information, The Consumer Experience (May 14, 2003); Workshop: Technologies for Protecting Personal Information, The Business Experience (June 4, 2003); Consumer Information Security Workshop (May 20, 2002).

[4] 69 Fed. Reg. 8538 (Feb. 24, 2004), <www.ftc.gov/os/2004/02/

[5] For the purposes of the workshop, the FTC Staff tentatively described spyware as "software that aids in gathering information about a person or organization without their knowledge and which may send such information to another entity without the consumer's consent, or asserts control over a computer without the consumer's knowledge." 69 Fed. Reg. 8538 (Feb. 24, 2004), <www.ftc.gov/os/2004/02/

defining spyware too broadly, some panelists at our workshop argued that the more prudent course is to focus on the harms caused by misuse or abuse of software rather than on the definition of spyware.

Panelists described a number of harms caused by spyware. These include invasions of privacy, security risks, and functionality problems for consumers. For example, spyware may harvest personally identifiable information from consumers through monitoring computer use without consent. Spyware also may facilitate identity theft by surreptitiously planting a keystroke logger on a consumer's personal computer. It may create security risks if it exposes communication channels to hackers. Spyware also may adversely affect the operation of personal computers, including slowing processing time and causing crashes, browser hijacking, home page resetting, installing dialers, and the like. These harms are problems in themselves, and could lead to a loss in consumer confidence in the Internet as a medium of communication and commerce.

Many of the panelists discussed how spyware may cause problems for businesses. Companies may incur costs as they seek to block and remove spyware from the computers of their employees. Employees will be less productive if spyware causes their computers to crash or they are distracted from their tasks by a barrage of pop-up ads. Spyware that captures the keystrokes of employees could be used to obtain trade secrets and other confidential information from businesses. In addition, representatives from companies such as ISPs, PC manufacturers, anti-virus providers, and an operating system manufacturer indicated that they spend substantial resources responding to customer inquiries when PCs or Internet browsers do not work as expected due to the presence of spyware. As such, these companies also may suffer injury to their reputations and lose good will.

Because of the relatively recent emergence of spyware, there has been little empirical data regarding the prevalence and magnitude of these problems for consumers and businesses. Given how broadly spyware can be distributed and the severity of some of its potential risks, government, industry, and consumers should treat the threats to privacy, security, and functionality posed by spyware as real and significant problems.

At the workshop, we heard that substantial efforts are currently underway to address spyware. Industry is deploying new technologies as well as distributing educational materials to assist consumers in addressing the problems associated with spyware. Similarly, at the workshop, industries involved with the dissemination of software reported that they are developing best practices.

Consumers and businesses are becoming more aware of the capabilities of spyware, and they are responding by installing anti-spyware products and taking other measures to minimize these risks. Government and industry-sponsored education programs, and industry self-regulation, could be instrumental in making users more aware of the risks of spyware, thereby assisting them in taking actions to protect themselves (such as running anti-spyware programs).[6]

FTC LAW ENFORCEMENT

As the nation's primary consumer protection agency, the Commission also has a law enforcement role to play in connection with unfair or deceptive acts or practices involved in the distribution or use of spyware.[7] At the workshop, FTC and DOJ staff members noted that many of the more egregious spyware practices described at the workshop may be subject to attack under existing Federal and State laws, and the workshop concluded with a request that industry and consumer groups notify the FTC staff of problematic practices.

The Commission is conducting non-public investigations related to the dissemination of spyware. As discussed at the workshop, however, investigating and prosecuting acts and practices related to spyware, particularly the more pernicious programs, pose substantial law enforcement challenges. Given the surreptitious nature of spyware, it often is difficult to ascertain from whom, from where, and how such products are disseminated. Consumer complaints, for instance, are less likely to lead

[6] Panelists at the workshop noted that consumers need to be very careful to obtain anti-spyware programs from legitimate providers because some purported anti-spyware programs in fact disseminate spyware.

[7] The Commission will find deception if there is a material representation, omission, or practice that is likely to mislead consumers acting reasonably in the circumstances, to their detriment. See Federal Trade Commission, Deception Policy Statement, appended to Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984) ("Deception Statement"). An act or practice is "unfair" if it causes or is likely to cause substantial injury to consumers, that injury is not outweighed by any countervailing benefits to consumers and competition, and consumers could not have reasonably avoided the injury. 15 U.S.C. § 45(n).

directly to targets than in other law enforcement investigations, because consumers often do not know that spyware has caused the problems or, even if they do, they may not know the source of the spyware.[8] Indeed, computer manufacturers stated at our workshop that they believe an increasing number of service calls are spyware-related and spyware-related issues are difficult to diagnose. Similarly, search engine providers testified that consumers complain to them, not realizing that the spyware (not the search engine) is causing their dissatisfaction with their search engine.

The Commission has long been active in challenging unfair or deceptive acts or practices on the Internet, and spyware cases are not fundamentally different. Over the course of nearly a decade, we have brought approximately 300 cases challenging Internet practices involving substantial consumer harms, including harms similar to those posed by some examples of spyware.

Most recently, in D Squared Solutions, LLC, the defendants allegedly exploited an operating system feature to harm consumers. The Windows operating system uses "Messenger Service" windows to allow network administrators to provide instant information to network users, for example, a message to let users know that a print job has been completed. The defendants in D Squared exploited this feature to send Messenger Service pop-up ads to consumers, advertising software that supposedly would block such ads in the future. Consumers would receive these pop-up ads as often as every ten minutes. The Commission filed a complaint in federal court alleging that the defendants unfairly interfered with consumers' use of their computers and tried to coerce consumers into buying software to block pop-up ads.[9]

The Commission brought several cases challenging the surreptitious distribution of dialer programs. A paper submitted at the workshop by the Computer Software Working Group[10] identified surreptitious downloads as an example of one of the problematic practices of some spyware programs. Past Commission actions have attacked similar programs that secretly disconnect consumers from their Internet Service Providers, reconnect them to another network, and charge them exorbitant fees for long distance telephone service or entertainment services delivered over the telephone line.[11] We also have challenged the practice of "pagejacking" consumers and then "mousetrapping" them at pornographic web sites.[12] These cases demonstrate that the Commission has the authority under Section 5 of the FTC Act to take action to prevent harms to consumers similar to those that spyware allegedly causes.

CONCLUSION

Spyware appears to be a new and rapidly growing practice that poses a risk of serious harm to consumers. The Commission is learning more about this practice, so that government responses to spyware will be focused and effective. We are continuing to pursue law enforcement investigations. The FTC thanks this Committee for focusing attention on this important issue, and for giving us an opportunity to present the preliminary results from our workshop. We look forward to further discussions with the Subcommittee on this issue.

Mr. STEARNS. Thank you, Commissioner. Mr. Howard Beales, Director of Bureau of Consumer Protection.

## STATEMENT OF HON. J. HOWARD BEALES III

Mr. BEALES. Thank you, Mr. Chairman, and members of the subcommittee. I'd like to thank you for providing the Federal Trade Commission with this opportunity to submit testimony. The writ-

[8] Identifying the source of spyware is especially difficult when consumers were not even aware that the spyware had been installed.

[9] FTC v. D Squared Solutions, LLC, No. 03-CV-3108 (D. Md. 2003). The case is currently in litigation.

[10] The Consumer Software Working Group is comprised of public interest groups, software companies, Internet Service Providers, hardware manufacturers, and others. Available at <http://www.cdt.org/privacy/spyware/2

[11] See, e.g., FTC v. Alyon Technologies, Inc., No. 1:03-CV-1297 (N.D. Ga. 2003); FTC v. BTV Indus., No. CV-S-02-0437-LRH-PAL (D. Nev. 2003); FTC v. Anderson, No. C00-1843P (W.D. Wash. 2000); FTC v. RJB Telcom, Inc., No. 002017 PHX EHC (D. Az. 2000); FTC v. Sheinkin, No. 2-00-3636 18 (D.S.C. 2000); FTC v. Verity Int'l, Ltd., No. 00 Civ. 7422 (LAK) (S.D.N.Y. 2000); FTC v. Audiotex Connection, Inc., No. CV-97-00726 (E.D.N.Y. 1997); see also Beylen Telecom, Ltd., FTC Docket No. C-3782 (final consent Jan. 23, 1998).

[12] See, e.g., FTC v. Zuccarini, No. 01-CV-4854 (E.D. Pa. 2002); FTC v. Carlos Pereira d/b/a atariz.com, No. 99-1367-A (E.D.N.Y. 1999).

ten testimony represents the views of the Federal Trade Commission and my oral comments do not necessarily reflect the views of the Commission or any individual Commissioner.

We're here today to discuss spyware, a subject of growing concern to consumers. Loosely defined, spyware is software that aids in gathering information about a person or organization without their knowledge and it may send such information to another entity without the consumers consent. Other spyware may assert control over a computer without the consumer's knowledge.

As in many cases of the new internet issues, the question is how to proceed against practices that are clearly abusive without interfering with the benefits that the internet provides to consumers. As Commissioner Thompson has described, we've accomplished this task through a series of workshops and hearings where the Commission has sought to understand the online marketplace and its information practices, to assess the impact of these practices on consumers, and to challenge industry leaders to deal with consumers in a straight forward and responsible manner.

Our most recently application of this approach was last week's workshop, monitoring software on your PC, spyware, adware and other software. It seems clear from the workshop's discussion that spyware may harvest personally identifiable information from consumers through monitoring computer use without consent. It also may facilitate identity theft by surreptitiously planting a keystroke logger on a user's personal computer. Spyware may create security risks if it exposes communications' channels to hackers. It also may affect the operation of personal computers, causing crashes, browser hijacking, home page resetting and the like.

These harms are problems in themselves and could lead to a loss in consumer confidence in the internet as a medium of communication and commerce.

Second, many of the panelists discussed how spyware may cause problems for businesses too. Companies may incur costs as they seek to block and remove spyware from computers of their employees or their customers. Employees will also be less productive if spyware causes their computers to crash or if they're distracted from their tasks by a barrage of popup ads. Spyware that captures the keystrokes of employees could be used to obtain trade secrets and confidential information from businesses.

We also heard that substantial efforts are currently underway to address spyware. In response to market forces, industry is developing and deploying new technologies to assist consumers. Consumers and businesses are becoming more aware of the risks of spyware and they're responding by installing anti-spyware products and other measures. Certain industry representatives indicated that they would explore best practices and consumer education on issues related to spyware. All of these efforts are very encouraging.

Another key theme of our workshop was the need to define the problem carefully and clearly. Defining a class of software that causes problems is a difficult task. Spyware is an elastic and vague term that's been used to describe a wide range of software. A vague definition of software could be so broad that it covers software that is beneficial or benign, software that is harmful, software that is beneficial or benign, but misused, and software that is just poorly

written or inefficient code. Such imprecise definitions would treat these types of software in the same manner. We need to determine whether there is a definable class of software that can truly be called spyware.

The easiest way to start drawing lines is through case by case law enforcement. The Commission has law enforcement authority to challenge unfair or deceptive practices involved in the distribution or use of spyware. At the workshop, FTC and DOJ staff members noted that many of the more egregious spyware practices described at the workshop are subject to attack under existing Federal and State laws including Section 5 of the FTC Act.

We have nonpublic investigations related to the dissemination of spyware. However, investigating and prosecuting acts and practices related to spyware, particularly the more pernicious programs pose law enforcement challenges. Given the surreptitious nature of spyware, it is often difficult to ascertain from whom, from where and how such products are dissemination. Consumer complaints are less likely to lead directly to targets that are in other law enforcement investigations because consumers often do not know that spyware has caused their problems. Even if they do, they may not know the source of the spyware.

Despite the obstacles, the FTC has been active in taking action against internet practices involving consumer injury similar to those caused by spyware. For example, we're currently litigating against defendants who exploited allegedly an operating system feature to send incessant messenger service popup ads to consumers. It advertised software that supposedly would block such ads in the future. We filed a complaint, alleging that the defendants unfairly interfered with consumers' use of their computers and tried to coerce consumers into buying software to block the popup ads.

And we brought several cases challenging the surreptitious distribution of dialer programs. These programs secretly disconnect consumers from their ISPs, reconnect them to another network and then charge exorbitant fees for long-distance telephone service or entertainment services delivered over the telephone line.

We've also challenged the practice of page-jacking and then mouse-trapping consumers at pornographic websites. And the practice of bombarding consumers with an endless sequence of popup ads. We have the legal tools necessary to address bad practices.

We continue to remain vigilant and eager to take action against those who are engaged in bad practices, and we've asked industry and consumer groups to notify the FTC staff of problematic practices. We are, as we said at the workshop, taking names.

Thank you and I look forward to answering any questions that you may have.

[The prepared statement of Hon. J. Howard Beales III follows:]

## PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION

Mr. Chairman and members of the Committee, the Federal Trade Commission ("Commission" or "FTC") appreciates this opportunity to provide the Commission's views on "spyware." [1]

The FTC has a broad mandate to prevent unfair competition and unfair or deceptive acts or practices in the marketplace. Section 5 of the Federal Trade Commission Act gives the agency the authority to challenge acts and practices in or affecting commerce that are unfair or deceptive.[2] The Commission's law enforcement activities against unfair or deceptive acts and practices are generally designed to promote informed consumer choice. This statement will discuss the FTC's activities related to spyware, including our recent workshop and potential law enforcement actions.

### FTC SPYWARE WORKSHOP

For nearly a decade, the FTC has addressed online privacy and security issues affecting consumers. Through a series of workshops and hearings, the Commission has sought to understand the online marketplace and its information practices, to assess the impact of these practices on consumers, and to challenge industry leaders to develop and implement meaningful self-regulatory programs.[3]

The most recent example of this approach is the workshop entitled "Monitoring Software on Your PC: Spyware, Adware, and Other Software" that was held last week. The workshop was designed to provide us with information about the nature and extent of problems related to spyware, and possible responses to those problems. Specifically, the workshop focused on four main topics: (1) defining "spyware" and exploring how it is distributed (including the role of peer-to-peer file-sharing software and whether spyware may differ from "adware"); (2) examining spyware's general effects on consumers and competition; (3) exploring spyware's potential security and privacy risks; and (4) identifying technological solutions, industry initiatives, and governmental responses (including consumer education) related to spyware. Underscoring the importance of this issue both FTC Commissioners Orson Swindle and Mozelle Thompson personally participated in the workshop.

To encourage broad-based participation, the FTC issued a Federal Register Notice announcing the workshop and requesting public comment.[4] The Commission received approximately 200 comments, and the record will remain open until May 21, 2004, for submission of additional comments. At the workshop, a wide range of panelists engaged in a spirited debate concerning spyware, including what government, industry, and consumers ought to do to respond to the risks associated with spyware.

Although the agency is continuing to receive information on this important issue, the record at the workshop leads to some preliminary conclusions. First, perhaps the most challenging task is to carefully and clearly define the issue. "Spyware" is an elastic and vague term that has been used to describe a wide range of software.[5] Some definitions of spyware could be so broad that they cover software that is beneficial or benign; software that is beneficial but misused; or software that is just poorly written or has inefficient code. Indeed, there continues to be considerable debate regarding whether "adware" should be considered spyware. Given the risks of defining spyware too broadly, some panelists at our workshop argued that the more prudent course is to focus on the harms caused by misuse or abuse of software rather than on the definition of spyware.

Panelists described a number of harms caused by spyware. These include invasions of privacy, security risks, and functionality problems for consumers. For example, spyware may harvest personally identifiable information from consumers through monitoring computer use without consent. Spyware also may facilitate identity theft by surreptitiously planting a keystroke logger on a consumer's personal computer. It may create security risks if it exposes communication channels to hack-

---

[1] The written statement presents the views of the Federal Trade Commission. Oral statements and responses to questions reflect the views of the speaker and do not necessarily reflect the views of the Commission or any other Commissioner.

[2] 15 U.S.C. § 45.

[3] *See, e.g., Workshop: Technologies for Protecting Personal Information, The Consumer Experience (May 14, 2003); Workshop: Technologies for Protecting Personal Information, The Business Experience* (June 4, 2003); *Consumer Information Security Workshop* (May 20, 2002).

[4] 69 Fed. Reg. 8538 (Feb. 24, 2004), <www.ftc.gov/os/2004/02/

[5] For the purposes of the workshop, the FTC Staff tentatively described spyware as "software that aids in gathering information about a person or organization without their knowledge and which may send such information to another entity without the consumer's consent, or asserts control over a computer without the consumer's knowledge." 69 Fed. Reg. 8538 (Feb. 24, 2004), <www.ftc.gov/os/2004/02/

ers. Spyware also may adversely affect the operation of personal computers, including slowing processing time and causing crashes, browser hijacking, home page resetting, installing dialers, and the like. These harms are problems in themselves, and could lead to a loss in consumer confidence in the Internet as a medium of communication and commerce.

Many of the panelists discussed how spyware may cause problems for businesses. Companies may incur costs as they seek to block and remove spyware from the computers of their employees. Employees will be less productive if spyware causes their computers to crash or they are distracted from their tasks by a barrage of pop-up ads. Spyware that captures the keystrokes of employees could be used to obtain trade secrets and other confidential information from businesses. In addition, representatives from companies such as ISPs, PC manufacturers, anti-virus providers, and an operating system manufacturer indicated that they spend substantial resources responding to customer inquiries when PCs or Internet browsers do not work as expected due to the presence of spyware. As such, these companies also may suffer injury to their reputations and lose good will.

Because of the relatively recent emergence of spyware, there has been little empirical data regarding the prevalence and magnitude of these problems for consumers and businesses. Given how broadly spyware can be distributed and the severity of some of its potential risks, government, industry, and consumers should treat the threats to privacy, security, and functionality posed by spyware as real and significant problems.

At the workshop, we heard that substantial efforts are currently underway to address spyware. Industry is deploying new technologies as well as distributing educational materials to assist consumers in addressing the problems associated with spyware. Similarly, at the workshop, industries involved with the dissemination of software reported that they are developing best practices.

Consumers and businesses are becoming more aware of the capabilities of spyware, and they are responding by installing anti-spyware products and taking other measures to minimize these risks. Government and industry-sponsored education programs, and industry self-regulation, could be instrumental in making users more aware of the risks of spyware, thereby assisting them in taking actions to protect themselves (such as running anti-spyware programs).[6]

FTC LAW ENFORCEMENT

As the nation's primary consumer protection agency, the Commission also has a law enforcement role to play in connection with unfair or deceptive acts or practices involved in the distribution or use of spyware.[7] At the workshop, FTC and DOJ staff members noted that many of the more egregious spyware practices described at the workshop may be subject to attack under existing Federal and State laws, and the workshop concluded with a request that industry and consumer groups notify the FTC staff of problematic practices.

The Commission is conducting non-public investigations related to the dissemination of spyware. As discussed at the workshop, however, investigating and prosecuting acts and practices related to spyware, particularly the more pernicious programs, pose substantial law enforcement challenges. Given the surreptitious nature of spyware, it often is difficult to ascertain from whom, from where, and how such products are disseminated. Consumer complaints, for instance, are less likely to lead directly to targets than in other law enforcement investigations, because consumers often do not know that spyware has caused the problems or, even if they do, they may not know the source of the spyware.[8] Indeed, computer manufacturers stated at our workshop that they believe an increasing number of service calls are spyware-related and spyware-related issues are difficult to diagnose. Similarly, search engine providers testified that consumers complain to them, not realizing

[6] Panelists at the workshop noted that consumers need to be very careful to obtain anti-spyware programs from legitimate providers because some purported anti-spyware programs in fact disseminate spyware.

[7] The Commission will find deception if there is a material representation, omission, or practice that is likely to mislead consumers acting reasonably in the circumstances, to their detriment. *See* Federal Trade Commission, Deception Policy Statement, *appended to Cliffdale Assocs., Inc.,* 103 F.T.C. 110, 174 (1984) ("Deception Statement"). An act or practice is "unfair" if it causes or is likely to cause substantial injury to consumers, that injury is not outweighed by any countervailing benefits to consumers and competition, and consumers could not have reasonably avoided the injury. 15 U.S.C. § 45(n).

[8] Identifying the source of spyware is especially difficult when consumers were not even aware that the spyware had been installed.

that the spyware (not the search engine) is causing their dissatisfaction with their search engine.

The Commission has long been active in challenging unfair or deceptive acts or practices on the Internet, and spyware cases are not fundamentally different. Over the course of nearly a decade, we have brought approximately 300 cases challenging Internet practices involving substantial consumer harms, including harms similar to those posed by some examples of spyware.

Most recently, in *D Squared Solutions, LLC,* the defendants allegedly exploited an operating system feature to harm consumers. The Windows operating system uses "Messenger Service" windows to allow network administrators to provide instant information to network users, for example, a message to let users know that a print job has been completed. The defendants in *D Squared* exploited this feature to send Messenger Service pop-up ads to consumers, advertising software that supposedly would block such ads in the future. Consumers would receive these pop-up ads as often as every ten minutes. The Commission filed a complaint in federal court alleging that the defendants unfairly interfered with consumers' use of their computers and tried to coerce consumers into buying software to block pop-up ads.[9]

The Commission brought several cases challenging the surreptitious distribution of dialer programs. A paper submitted at the workshop by the Computer Software Working Group[10] identified surreptitious downloads as an example of one of the problematic practices of some spyware programs. Past Commission actions have attacked similar programs that secretly disconnect consumers from their Internet Service Providers, reconnect them to another network, and charge them exorbitant fees for long distance telephone service or entertainment services delivered over the telephone line.[11] We also have challenged the practice of "pagejacking" consumers and then "mousetrapping" them at pornographic web sites.[12] These cases demonstrate that the Commission has the authority under Section 5 of the FTC Act to take action to prevent harms to consumers similar to those that spyware allegedly causes.

CONCLUSION

Spyware appears to be a new and rapidly growing practice that poses a risk of serious harm to consumers. The Commission is learning more about this practice, so that government responses to spyware will be focused and effective. We are continuing to pursue law enforcement investigations. The FTC thanks this Committee for focusing attention on this important issue, and for giving us an opportunity to present the preliminary results from our workshop. We look forward to further discussions with the Subcommittee on this issue.

Mr. STEARNS. I thank you. Mr. Ari Schwartz, Associate Director, Center for Democracy and Technology.

Welcome.

## STATEMENT OF ARI SCHWARTZ

Mr. SCHWARTZ. Chairman Stearns, Ranking Member Schakowsky, members of the committee, thank you for inviting CDT to testify today.

In November, we released our first report on the spyware issue entitled "Ghosts in our Machines." At that same time we asked consumers to send us their concerns about specific spyware experiences. Since then hundreds have responded.

---

[9] *FTC v. D Squared Solutions, LLC,* No. 03-CV-3108 (D. Md. 2003). The case is currently in litigation.

[10] The Consumer Software Working Group is comprised of public interest groups, software companies, Internet Service Providers, hardware manufacturers, and others. *Available at* <http://www.cdt.org/privacy/spyware/20040419cswg.pdf>

[11] *See, e.g., FTC v. Alyon Technologies, Inc.,* No. 1:03-CV-1297 (N.D. Ga. 2003); *FTC v. BTV Indus.,* No. CV-S-02-0437-LRH-PAL (D. Nev. 2003); *FTC v. Anderson,* No. C00-1843P (W.D. Wash. 2000); *FTC v. RJB Telcom, Inc.,* No. 002017 PHX EHC (D. Az. 2000); *FTC v. Sheinkin,* No. 2-00-3636 18 (D.S.C. 2000); *FTC v. Verity Int'l, Ltd.,* No. 00 Civ. 7422 (LAK) (S.D.N.Y. 2000); *FTC v. Audiotex Connection, Inc.,* No. CV-97-00726 (E.D.N.Y. 1997); *see also Beylen Telecom, Ltd.,* FTC Docket No. C-3782 (final consent Jan. 23, 1998).

[12] *See, e.g., FTC v. Zuccarini,* No. 01-CV-4854 (E.D. Pa. 2002); *FTC v. Carlos Pereira d/b/a atariz.com,* No. 99-1367-A (E.D.N.Y. 1999).

Spyware is clearly an issue of growing concern for internet users. As we document in our report, the worse practices that we've seen are often based on mutated practices of legitimate software companies. Therefore, defining the term spyware has become difficult, if not impossible.

The basic problem of spyware is that software being created to run on users' computers, that they have no control over and do not want, including some software that passes on personal information about the computer user with their consent. CDT believes that in order to stop this growing problem, we will need to see action in three areas: enforcement of existing law, industry commitment to stopping bad practices, and legislation to protect privacy online.

I will quickly address each of these areas. It is CDT's opinion that many of the worst practices that we have seen today in the spyware are already illegal under existing fraud statutes. For example, if a consumer walked into a store and the door was locked behind them and they were forced to buy a product, we would expect law enforcement to do something about it. If hundreds of thousands of consumers were not allowed to leave a contract that they didn't even know that they'd enter, we would expect consumer law enforcement agencies to do something. And if a third party were to tamper with consumers' telephones in such a way that when they try to call Barnes and Noble they were instead connected to an adult book store, certainly we would expect law enforcement to be there. Yet, the online equivalent of each of these actions, online coercion, inability to uninstall or disable and host file overriding have not been a serious area of action for any law enforcement body to date.

CDT worked with consumer groups and industry to help develop examples of unfair, deceptive and devious practices involving software. These examples are based on real cases where CDT believes that law enforcement should be focusing its efforts. That full document was included as part of my written testimony.

Second, industry needs to do a better job of creating self-regulatory structures for software. CDT is encouraged by the advances in the anti-software technology such as those discussed here today by EarthLink and Microsoft and the others discussed at the FTC workshop last week. As we have seen in the spam war, it's very likely that as the anti-spyware technologies increase, the efforts of the spyware creators will undoubtedly double as well.

Industry should go further and start to draw clear lines in the spectrum of current behaviors to begin to help consumers to distinguish the good actors from the bad. A code of best practices could give consumers the information and ability that they need to make better decisions in the marketplace today.

Last, CDT strongly believes that many of the privacy concerns with spyware, some of which fall out of the scope of legal protections could be clearly addressed with the privacy law.

As the chairman and the committee know, CDT has long argued that until we have a privacy law that addresses all of the basic fair information practices that privacy issues that we first saw 8 years ago with the collection of information via the web and then with cookies and then with spam and now with spyware will continue. And it will repeat again in new technologies in the future.

A privacy law would get a root concern, not the root concern, but at a root concern rather than trying to define and scope each new technology in a limiting way. Still, spyware may pose some unique challenges that are not covered in the areas that I've outlined. We commend Representative Bono and Representative Towns for their work and their early attempts to take on this difficult issue, yet we also recognize that it would be difficult to define spyware or even the broader category of software in a way that addresses the problem without confining the market or accidentally legitimizing questionable practices that fall outside of the scope of the legislation.

CDT is committed to working with the committee as the efforts move forward and I look forward to answering all of your questions.

[The prepared statement of Ari Schwartz follows:]

PREPARED STATEMENT OF ARI SCHWARTZ, ASSOCIATE DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY

Chairman Sterns and Ranking Member Schakowsky, thank you for holding this hearing on spyware, an issue of growing concern for consumers and businesses alike. CDT is pleased to have the opportunity to participate.

CDT is a non-profit, public interest organization dedicated to preserving and promoting privacy and other democratic values and civil liberties on the Internet. CDT has been widely-recognized as a leader in the policy debate about the issues raised by so-called "spyware" applications.[1] We have been engaged in the early legislative, regulatory, and self-regulatory efforts to deal with the spyware problem, and have been active in public education efforts through the press and our own grassroots network.

**A. Summary**

In our testimony today, we hope to address two questions: What is spyware? And how should we respond to it?

In Section B of our testimony below, we attempt to help define and understand the spyware problem. CDT's report "Ghosts in Our Machines: Background and Policy Proposals on the 'Spyware' Problem,"[2] released in November 2003, addresses this issue. The report describes the range of invasive software applications referred to as "spyware" and clarifies the privacy, transparency and user control issues raised by these rogue programs.

Additionally, over the last six months, CDT has led discussions of a Consumer Software Working Group that includes leading members of the Internet industry, advertising companies, public interest groups and academics in order to identify examples the worst practices that consumers are facing online. In our testimony today, we highlight some of the pertinent issues raised by the working group, summarize the findings of CDT's report, and describe some of CDT's subsequent research and ongoing efforts in these areas.

In Section C, we turn to potential responses to the spyware problem. CDT sees three major areas where action is necessary to stem the disturbing trend toward a loss of control and transparency for Internet users:

---

[1] *See,* e.g., CDT's "Campaign Against Spyware," http://www.cdt.org/action/spyware/action (calling on users to report their problems with spyware to CDT; since November 2003, CDT has received over 250 responses). CDT's Complaint and Request for Investigation, Injunction, and Other Relief, in the Matter of MailWiper, Inc., and Seismic Entertainment Productions, Inc., February 11, 2004 (available at http://www.cdt.org/privacy/20040210cdt.pdf). "Eye Spyware," The Christian Science Monitor Editorial, April 21, 2004 ["Some computer-focused organizations, like the Center for Democracy and Technology, are working to increase public awareness of spyware and its risks. "The Spies in Your Computer," New York Times Editorial, February 18, 2004 (arguing that "Congress will miss the point (in spyware legislation) if it regulates specific varieties of spyware, only to watch the programs mutate into forms that evade narrowly tailored law. A better solution, as proposed recently by the Center for Democracy and Technology, is to develop privacy standards that protect computer users from all programs that covertly collect information that rightfully belongs to the user."). John Borland, "Spyware and its discontents," CNET.com, February 12, 2004. ("In the past few months, Ari Schwartz and the Washington, D.C.-based Center for Democracy andTechnology have leapt into the front ranks of the Net's spyware-fighters.")

[2] http://www.cdt.org/privacy/031100spyware.pdf

1) Enforcement of existing laws could go a long way toward reducing the problem of spyware. While longstanding fraud statutes already cover many of the issues raised by these applications, currently they are rarely enforced against spyware programmers and distributors.
2) Fundamental to the issue of spyware is the overarching concern about online Internet privacy. Legislation to address the collection and sharing of information on the Internet would resolve many of the privacy issues raised by spyware. If we do not deal with the broad Internet privacy concerns now, in the context of spyware, we will undoubtedly find ourselves confronted by them yet again when they are raised anew by some other, as yet unanticipated, technology.
3) To be effective, legislation and enforcement approaches will have to be carried out concurrently with better consumer education, industry self-regulation and the development of new anti-spyware technologies.

We address each of these avenues in turn.

**B. Defining and Understanding "Spyware" and "Adware"**

"Spyware" has no precise definition. The term has been applied to everything from keystroke loggers, to advertising applications that track users' web browsing, to web cookies, to programs designed to help provide security patches directly to users. "Spyware" programs can be installed on users' computers in a variety of ways, and they can have widely differing functionalities.

What these programs have in common is a lack of transparency and an absence of respect for users' ability to control their own computers and Internet connections.

While many programs that have been called "spyware" are advertising software, CDT has emphasized that there is nothing inherently objectionable about ad-support as a business model. We highlight email applications, such as Eudora, that are successful and user-friendly examples of ad-supported software.

However, in many cases, the revenue that these applications provide has given software distributors the incentive to push them onto users' computers using deceptive or fraudulent means. Ad-support can and must be implemented in a way that is transparent to users and respects their choices and privacy preferences.

**Distribution of Spyware**

"Spyware" programs can be distributed in a variety of ways. For example, they may be bundled with other free applications, including peer-to-peer file sharing applications; they may be distributed through deceptive download practices; or they may be installed by exploiting security holes in the web browser or operating system on a user's computer. In some cases, once one "spyware" application has gained access to a user's computer, it will surreptitiously download and install other applications.

In each of these scenarios, users generally do not know that the software is being installed. And once these invasive applications are on a user's computer they can be difficult or impossible to find and remove.

**Effects of Spyware**

As mentioned above, the overarching concerns raised by spyware applications are *transparency* and *user control.* Within these broad categories, spyware programs can raise a host of specific concerns.

- These programs can change the appearance of websites, modify users' "start" and "search" pages in their browsers, or change low level system settings. In our complaint to the FTC against MailWiper and Seismic Entertainment Productions, filed in February, CDT asked the Commission to investigate one particularly egregious example of such "browser hijacking" behavior.
- Spyware programs are also often responsible for significant reductions in computer performance and system stability. In many cases, consumers mistakenly assume that the problem is with another application or with their Internet provider, placing a substantial burden on the support departments of providers of those legitimate applications and services.
- Spyware programs can track users' online activities. Some gather personally identifiable information. The most egregious forms of spyware can capture all keystrokes, or record periodic screenshots from a user's computer.
- Even in cases where spyware programs transmit no personally identifiable information, their hidden, unauthorized appropriation of users' computing resources and Internet connections threatens the security of computers and the integrity of online communications. The "auto-update" component of many of these applications can create major new security vulnerabilities by including capabilities to automatically download and install additional pieces of code without noti-

fying users or asking for their consent, typically with minimal security safeguards.

CDT is currently conducting technical and public opinion research on the spyware issue. We hope to continue to report the results of this work to the Committee as we learn more.

**C. Possible Responses to Spyware Concerns**

Combating the most invasive spyware technologies will require a combination of approaches. First and foremost, vigorous enforcement of existing anti-fraud laws should result in a significant reduction of the spyware problem.

Addressing the problem of spyware also offers an important opportunity to establish in law baseline standards for privacy for online collection and sharing of data. Providing these protections would not only address the privacy concerns that current forms of spyware raise, but would put in place standards that would apply to future technologies that might challenge online privacy. Anti-spyware tools, better consumer education, and self-regulatory policies are also all necessary elements of a spyware solution.

Legislation to establish standards for privacy, notice, and consent specifically for software, such as H.R.2929, currently before this Committee, may play an important role as well. The challenge to such efforts is in crafting language that effectively addresses the spyware issue without unnecessarily burdening legitimate software developers or unintentionally hindering innovation.

So far the efforts to address the spyware issue are all in very preliminary stages. They will each require cooperation among government, private sector, and public interest initiatives.

**Enforcement of Existing Law**

CDT believes that three existing federal laws already prohibit many of the invasive or deceptive practices employed by malevolent software makers. Better enforcement of these statutes could have an immediate positive effect on the spyware problem.

Title 5 of the Federal Trade Commission Act is most directly applicable to the most common varieties of spyware. We believe that many of the more invasive forms of spyware discussed above clearly fall under the FTC's jurisdiction over unfair and deceptive trade practices. Some of these practices are highlighted in the Appendix—the Consumer Software Working Group's Examples of Unfair, Deceptive or Devious Practices Involving Software. To our knowledge, the FTC so far has not brought any major actions against spyware makers or spyware distributing companies. In February, CDT filed a complaint with the FTC against two companies for engaging in browser hijacking to display deceptive advertisements to consumers for software sold by one of the companies.[3]

We believe that one of the most immediate ways in which Congress could have a positive impact on the spyware problem is by directing the FTC to increase enforcement against unfair and deceptive practices in the use or distribution of downloadable software and by providing increased resources for such efforts.

Several laws besides the FTC Act may also have relevance. The Electronic Communications Privacy Act (ECPA), which makes illegal the interception of communications without a court order or permission of one of the parties, may cover programs that collect click-through data and other web browsing information without consent. The Computer Fraud and Abuse Act (CFAA) also applies to some uses of spyware. Distributing programs by exploiting security vulnerabilities in network software, co-opting control of users' computers, or exploiting their Internet connection can constitute violations of the CFAA, especially in cases where spyware programs are used to steal passwords and other information.

In addition to federal laws, many states have long-standing fraud statutes that would allow state attorneys general to take action against invasive or deceptive software. Like their federal counterparts, these laws have not been strongly enforced to date.

**New Legislation**

CDT has argued that the most effective way to address the spyware problem through legislation is in the context of online privacy generally. Specifically, we believe that the privacy dimension of spyware would best be addressed through baseline Internet privacy legislation that is applicable to online information collection

[3] Complaint and Request for Investigation, Injunction, and Other Relief, in the Matter of MailWiper, Inc., and Seismic Entertainment Productions, Inc., February 11, 2004 (available at http://www.cdt.org/privacy/20040210cdt.pdf).

and sharing irrespective of the technology or application. CDT has advocated such legislation before the Senate Commerce Committee and in other fora. Until we address the online privacy concern, new privacy issues will arise as we encounter new online technologies and applications.

Still, software may pose some unique problems. A comprehensive legislative solution to spyware may need to address the user-control aspects of the issue such as piggybacking, and avoiding uninstallation. H.R. 2929 before this Committee represents an important acknowledgement of several of these problems. We appreciate the desire to craft targeted legislation focusing on some of the specific problems raised by spyware, and CDT commends Representatives Bono and Towns for bringing attention to this important issue.

At the same time, we wish to emphasize the complexity of such efforts. The broad industry opposition to an anti-spyware bill recently passed in the Utah legislature, based on potential unintended consequences of the bill for legitimate software companies, demonstrates the difficulties that can be introduced by such legislation if it is not carefully drafted. We know Representatives Bono and Towns have been looking hard at some of the specific definitional concerns raised by CDT and others, and we look forward to continuing to work with the Committee on this bill.

**Non-Regulatory Approaches**

Technology measures, self-regulation and user education must work in concert, and will be critical components of any spyware solution. Companies must do a better job of helping users understand and control how their computers and Internet connections are used, and users must become better educated about how to protect themselves from spyware.

The first step is development of industry best practices for downloadable software. Although not all software manufacturers will abide by best practices, certification programs will allow consumers to quickly identify those that do and to avoid those that do not. In the current environment consumers cannot easily determine which programs post a threat, especially as doing so can involve wading through long and unwieldy licensing agreements.

Technologies to deal with invasive applications and related privacy issues are in various stages of development. Several programs exist that will search a hard-drive for these applications and attempt to delete them. Some companies are experimenting with ways to prevent installation of the programs in the first place. However, even these technologies encounter difficulties in determining which applications to block or remove. Clear industry best practices are crucial in this regard as well.

Standards such as the Platform for Privacy Preferences (P3P) may also play an important role in technical efforts to increase transparency and provide users with greater control over their computers and their personal information. P3P is a specification developed by the World Wide Web Consortium (W3C) to allow websites to publish standard, machine-readable statements of their privacy policies for easy access by a user's browser. If developed further, standards like P3P could help facilitate privacy best practices to allow users and anti-spyware technologies distinguish legitimate software from unwanted or invasive applications.

The IT industry has initially been slow to undertake such efforts. However, increasing public concern about spyware and the growing burden placed on the providers of legitimate software by these invasive applications has led to more industry attention on this front.[4] The Consumer Software Working Group, including major Internet service providers, software companies, and hardware manufacturers, has expressed its view that this area is ripe for industry self-regulation and best practices.

CDT believes Congress can have an immediate positive impact by encouraging industry to continue to follow through on these efforts.

**D. Conclusion**

Users should have control over what programs are installed on their computers and over how their Internet connections are used. They should be able to rely on a predictable web-browsing experience and to remove for any reason and at any

[4] See, e.g. , Earthlink press release: Earthlink Offers Free Spyware Analysis Tool to All Internet Users, January 14, 2004 (available at: http://www.earthlink.net/about/press/pr_analysis/); America Online press release: America Online Announces Spyware Protection for Members, January 6, 2004 (available at: http://media.aoltimewarner.com/media/newmedia/cb_press_view.cfm?release_num=55253697); Microsoft press release: Battling 'Spyware': Debate Intensifies on Controlling Deceptive Programs, April 20, 2004 (available at: http://www.microsoft.com/presspass/features/2004/apr04/04-20Spyware.asp)

time programs they don't want. The widespread proliferation of invasive software applications takes away this control.

Better consumer education, industry self-regulation, and new anti-spyware tools are all key to addressing this problem. New laws, if carefully crafted, may also have a role to play. Many spyware practices, however, are already illegal. Even before passing new legislation, existing fraud statutes should be robustly enforced against the distributors of these programs.

The potential of the Internet will be substantially harmed if users come to believe that they cannot use the Internet without being at risk of infection from spyware applications. We must find creative ways to address this problem through law, technology, public education and industry initiatives if the Internet is to continue to flourish.

## APPENDIX: EXAMPLES OF UNFAIR, DECEPTIVE OR DEVIOUS PRACTICES INVOLVING SOFTWARE

### CONSUMER SOFTWARE WORKING GROUP

The Consumer Software Working Group is a diverse community of public interest groups, software companies, Internet service providers, hardware manufacturers, and others that are seeking consensus responses to the concerns raised by practices that harm consumers.

Over the past several years, a subset of computer software referred to as "spyware" has become the subject of growing public concern. Computer users increasingly find programs on their computers that they did not know were installed, that create risks to privacy, that open security holes, that impair the performance and stability of their systems, that frustrate their attempts to uninstall or disable the programs, or that lead them to mistakenly believe that these problems are the fault of another application or their Internet service provider.

There is agreement that these practices can raise serious concerns. At the same time, the wide range of and lack of clarity in attempted definitions for the types of software practices that most concern consumers hamper attempts at self-regulatory, technological and legislative responses. Many definitions of spyware in circulation today are either under-inclusive in important respects or, more commonly, overbroad so that they include practices that clearly benefit consumers, or both.[5]

The Center for Democracy and Technology convened the Consumer Software Working Group. Companies, public interest groups or academics interested in joining the Working Group should contact Ari Schwartz <ari@cdt.org>, Michael Steffen <msteffen@cdt.org>, or John Morris <jmorris@cdt.org> at the Center for Democracy and Technology.

### EXAMPLES OF UNFAIR, DECEPTIVE OR DEVIOUS PRACTICES INVOLVING SOFTWARE VERSION 1.0

The Consumer Software Working Group is concerned about a specific set of devious, deceptive or unfair practices that adversely affect consumers online. While the following list of examples is not nearly complete, it describes a series of activities and behaviors that the Group considers to be clearly objectionable.

Specifically, the Group identifies three broad types of practices where abuses occur today. Most of these practices may be illegal under current law, depending on the specific facts of the particular case. Within each area, we offer illustrative examples, based on real cases. We note that each of the objectionable behaviors we identify has constructive consumer-friendly counterparts when carried out with proper notice and consent and in ways that give consumers control. Automatic installation, personalization and tracking, and in some cases resistance to uninstallation can provide important benefits to consumers.

We hope that this list of objectionable practices will help to focus technical, self-regulatory, regulatory and law enforcement efforts to protect consumers from inappropriate activities in a more targeted and effective manner, while avoiding unintended negative consequences for good actors and consumers alike. The Working Group believes that this is an area that could be ripe for self-regulatory efforts to craft industry principles to protect consumers and the marketplace.

1) **Hijacking**—The practices described in this section are objectionable to the extent that they enable an unaffiliated person to use the user's computer in a way

[5] For example, the Working Group observes that the current Utah law addresses practices involving software that most informed consumers would not consider unfair, deceptive or devious and fails to cover some practices that most informed consumers would consider unfair, deceptive or devious.

that ordinarily would not be expected. This may occur through an unnoticed program consuming the user's computing resources or resetting a user's existing configurations without the user's knowledge, or through coercion or deception.

Example: A computer user sees an Internet advertisement for Program A. The user clicks on the ad and is sent to a page that pops up a window asking if the user wants to download Program A. The user clicks "no," but Program A is eventually downloaded and installed anyway.

Example: A computer user sees an Internet advertisement for Product B. The user clicks on the advertisement, and is sent to a page that informs the user that "Program C is needed to view this Web page." This leads the user to believe that Program C is necessary to view the site about Product B, so the user clicks "yes" and the program is downloaded and installed. In fact, Program C is not necessary to view the website for Product B and the user is never informed of the actual reason why Program C was installed.

Example: A computer user sees an Internet advertisement for Program D. The user clicks on the ad, and she is sent to a page that immediately pops up a window asking if she wants to download Program D. The user clicks "no." This happens repeatedly until the user gets frustrated and clicks "yes."

Example: A computer user receives an Internet advertisement for Product E as part of a webpage he is looking at. Simply as a result of loading the ad, Software Program F wholly unrelated to Product E is downloaded onto the user's computer. No notice or opportunity to consent to download Software Program F was provided.

Example: While browsing the Internet, a computer user is offered the opportunity to download and install Software Program G. Using a fraudulently obtained digital certificate, the download request falsely identifies Software Program G as being from the user's trusted Internet Service Provider, H. In fact, the Program is not from Internet Service Provider H, and has no relation to the ISP. However, based on its claimed affiliation with H, the user agrees to let the program be downloaded and installed.

Example: A computer user loads Company I's Web page. The Web page opens another page running a java script. When the user closes Company I's Web page, the java script page covertly resets the user's homepage without obtaining consent.

Example: A computer user loads Company J's Web page. The Web page opens another page running a java script. When the user closes Company J's Web page, the java script page covertly resets the user's homepage. The java script is written such that any time the user attempts to reset his homepage, the program automatically resets it again so the user cannot reset his homepage to what it was before the hijacking took place.

Example: A computer user downloads Software Package K. Among the programs in Software Package K is a dialer application that was not mentioned in any advertisements, software licenses, or consumer notices associated with the package or in information provided in conjunction with the ongoing operations of the package. The dialer application is not an integral part of Software Package K. When the user opens her Web browser after installation of Software Package K, the dialer opens in a hidden window, turns off the sound of the user's computer, and calls a phone number without the user's permission.

Example: A computer user is sent Software Package L as an attachment to an unsolicited commercial email message. There is no documentation for Software Package L. Included in Software Package L is Program M that sends a message to Computer N. Computer N then uses Program M on the user's computer as a means to send out unsolicited commercial emails.

2) **Surreptitious surveillance**—The practices described in this section are objectionable to the extent that they involve intrusive and surreptitious collection and use of personally identifiable information about users that is wholly unrelated to the purpose of the software as described to the consumer.

Example: A computer user downloads Software Package P. Software Package P contains a keystroke logger unrelated to any functions described to the user. The keystroke logger records all information input on the user's computer and sends this information on to another computer user. The first user is not informed about the operation of the keystroke logger.

Example: Program Q advertises itself as a search tool bar. A user downloads Program Q to gain the search functionalities. Program Q installs a tool bar, but—once installed—also mines the user's registry and other programs for personally identifiable information about the user unrelated to the search functionality and without informing the user or obtaining consent. When the

user connects to the Internet, Program Q sends this information back to the company that makes Program Q.

3) **Inhibiting termination**—The practices described in this section are objectionable to the extent that they frustrate consumers' efforts to remove a program, deactivate it or otherwise render it inoperative. Generally, these practices are intended to prevent the user from severing or terminating a relationship with the provider of the program.

Example: A computer user downloads Software Package S. Software Package S contains Advertising Program T. Advertising Program T sends the user pop-up ads while the user is surfing the Web even if no other programs in Software Package S are running. The pop-up ads are not labeled as related to Advertising Program T or Software Package S in any way and there is no other way to find the ads' origin. The user is concerned about the increase in pop-up ads, but does not know whether they are caused by Program T or are from the Web sites that he is visiting. The user has no means to find out the origin of the ads in order to make a decision about uninstalling Program T.

Example: A computer user downloads Software Package U. As initially disclosed to the user, Software Package U contains a mandatory program, Advertising Program V, which is bundled as a way to generate revenue and pay for the development of Software Package U only. When the user uninstalls Software Package U, the user is not given a clear opportunity to uninstall Program V at that time, and Advertising Program V stays on the user's computer.

Example: A computer user downloads Gaming Program W. The user wants to remove Gaming Program W from the computer. Gaming Program W does not have an uninstall program or instructions and does not show up in the standard feature in the user's operating system that removes unwanted programs (assuming this feature exists in the operating system). The user's attempts to otherwise delete Program W are met by confusing prompts from Program W with misrepresentative statements that deleting the program will make all future operations unstable.

Example: A computer user downloads Program X. The user wants to remove Program X from the computer. Program X appears in the standard feature in the user's operating system that removes unwanted programs. However, when the user utilizes the "remove" option in the operating system, a component of Program X remains behind. The next time the user connects to the Internet, this component re-downloads the remainder of Program X and reinstalls it.

The following companies, organizations and individuals have worked to describe Examples of Unfair, Deceptive and Devious Practices Involving Software. These descriptions can be used to help focus technical, self-regulatory, regulatory and law enforcement efforts to protect consumers from inappropriate activities.

America Online; Business Software Alliance; Center for Democracy and Technology; Claria Corporation; Consortium of Anti-Spyware Technology Vendors; Consumer Action; CryptoRights Foundation; Dell, Inc.; Distributed Computing Industry Association; EarthLink; eBay; Electronic Frontier Foundation; Google; HP; Information Technology Industry Council; Internet Commerce Coalition; Lavasoft; Microsoft; Network Advertising Initiative; Privacilla.org; Sharman Networks; Peter Swire, Moritz College of Law of the Ohio State University;[6] TRUSTe; Webroot Software; WhenU; and Yahoo!.

Mr. STEARNS. I thank the gentleman. I'll start out with my line of questioning and I think I'll just make a general comment and then I want to ask each of you a specific question, a yes or no answer, if possible.

I think as in the opening statement of the chairman of our committee, the gentleman from Texas, indicated we found on employees in the Commerce Committee have over 200 spyware and they did not know this. We've heard from other members how it's affected their computers at home and slowed them down. So obviously, there's some deep concern, not only about privacy, but efficiency and overall security.

So the question is and I think I know the answers listening to your opening statements, I'll start with you, Commissioner. You at

[6] Individuals are listed with their affiliation for identification purposes only.

this point do not believe that we need legislation, just yes or no, is that true?

Mr. THOMPSON. Yes, at this time, we do not——

Mr. STEARNS. We do not need legislation. And Mr. Beales, do you think we need legislation?

Mr. BEALES. I do not.

Mr. STEARNS. And Mr. Schwartz?

Mr. SCHWARTZ. I think that we need privacy legislation today and we may need spyware legislation in the future once we've gone further in going after worst practices.

Mr. STEARNS. You mentioned three areas: enforcement, eliminating bad practices and legislation.

Mr. SCHWARTZ. And privacy legislation.

Mr. STEARNS. So what you're talking about is an overall privacy legislation of which spyware would be a component, is that what you're saying?

Mr. SCHWARTZ. That's correct, yes.

Mr. STEARNS. And Mr. Baker? Do we need legislation?

Mr. BAKER. We think legislation would complement industry technology efforts and FTC enforcement.

Mr. STEARNS. Okay, and Mr. Friedberg?

Mr. FRIEDBERG. Yes. We believe in a holistic solution and to the degree enforcement can't do what they need to do because there's some laws missing, then we would——

Mr. STEARNS. You mentioned you're going to have a new software program, but today, would you advocate legislation to solve this problem, yes or no?

Mr. FRIEDBERG. Again, I think it goes back to whether or not there's enough teeth in the existing laws to go after the deceptive practices.

Mr. STEARNS. Do you think there's enough teeth in the existing laws?

Mr. FRIEDBERG. Unfortunately, I'm not a lawyer, but I would——

Mr. STEARNS. I'm asking you a personal opinion. I mean you're here, you're one of the experts here on the panel and your high technology of interest and expertise, we've just told you that member employees on our Commerce Committee have over 200 of these spywares that they didn't know it, it's slowing it down, so you're saying that your software would solve all the problems?

Mr. FRIEDBERG. No, absolutely not.

Mr. STEARNS. Do you think legislation——

Mr. FRIEDBERG. We think there's a holistic strategy and I think Commissioner Thompson and others have stated they feel very confident about the current laws. That's fantastic, I think. We can go after them and create a deterrent, it's wonderful.

Mr. STEARNS. Let me ask you then, you testified that any Federal legislation should address deceptive behavior and not functionality and I guess that's the key point, that we want to not bog down the internet. We want to have the functionality there, but we've got to address this deceptive behavior.

Please explain what behaviors are not illegal already that we should address.

Mr. FRIEDBERG. Not illegal already?

Mr. STEARNS. In other words, when a person is dealing with spyware, from what I hear it looks like most of it is coming in illegally. It's in my computer and I don't want it. So that's a behavior that I don't want. So what is the functionality of this that I should allow it to be in and why shouldn't I legislate to say don't come in without my permission.

Mr. FRIEDBERG. When you actually look at the features that underlie some of what's happening, it turns out that a lot of those features have positive user benefit. For example——

Mr. STEARNS. Give me some examples of positive user benefit.

Mr. FRIEDBERG. Let's just take adware. Obviously, it's a very contentious issue, but a piece of software that's going to display some advertisements, that's what it does. That's its function. Now if I'm a user and I have to pay $120 a year for a service and I have the choice to maybe see some ads and not have to pay that money, I think that's a fair horse trade providing I was told up front what that deal is and I can fully understand the terms under which it's happening and so there's an example of where the feature is not the issue, it's when people do it deceptively where you have no control over that adware, it's just showing up in your box, can't turn it off. Clearly a bad situation.

Mr. STEARNS. Commissioner, you are on the panel of peers to be the strongest advocate for no legislation. The State of Utah has passed a bill. California and Texas is doing this. New York is going to do this. Shouldn't Congress, if nothing else, preempt these with a Federal law instead of having 50 separate State laws dealing with spyware?

Mr. THOMPSON. I understand that point and I think that——

Mr. STEARNS. I mean, the practicality.

Mr. THOMPSON. But what I say is at this time what I'm looking for is industry to define good behavior to isolate bad behavior. That's what you heard with the other people on this panel. There are certain behaviors that are bad that we can get at right now. Unfair and deceptive practices, for example, if they put something on your computer and it violates their privacy policy, then we can do something about it. If it's sending information that you have no way of avoiding, that's something we need to know about. But——

Mr. STEARNS. But shouldn't we stop that practice of putting it in your computer without you knowing about it?

Mr. THOMPSON. I think we can get at some of that right now. The point is that I need——

Mr. STEARNS. Well, why isn't our staff doing it? The public obviously has ignorance on this and doesn't even know. You click a bar up here, some of the bars that were clicked up here you hit cancel or yes or even the top of the dialog bar, it doesn't matter. You're still going to get the spyware in the computer, so tell me why shouldn't we stop that?

Mr. THOMPSON. And that's part of the challenge that we have. First of all, we need the responsible companies to come clean and tell consumers what it is they're doing, how they're doing it and then the second thing, then we need to isolate those people who are not.

Let me tell you something. Most of the people who are involved in the most insidious behavior, secret spyware that will get after,

that will allow them to get identity theft, to mine your information, etcetera, that's unlawful now and those people don't care about the law.

Mr. STEARNS. I'll conclude by just saying I'm a little concerned that you're not outraged that people have access to somebody's privacy, Social Security Numbers and all this and you're saying just let things go by the wayside when actually I would think you as Federal Trade Commission should be saying we need more money, we want to enforce it, we're going to do something about this, Congress, this is what we need.

Mr. THOMPSON. I am outraged and we always need more money, but what I am saying to you is there's a danger. The danger in trying to define this in the scope of legislation right now, is to be overbroad which will deny us of beneficial uses.

Mr. STEARNS. My time is up.

Mr. THOMPSON. Or too narrow.

Mr. STEARNS. The gentlelady, Ms. Schakowsky.

Ms. SCHAKOWSKY. Mr. Thompson, if legislation is not warranted at this time, I know you had a workshop and that's the beginning, but what are you doing exactly in terms of enforcement of current laws? It seems to me the ball is in your court as well as in that of industry. You're looking for a voluntary industry response, you're saying, but what exactly are your plans then in the short term?

Mr. THOMPSON. I would like the Bureau Director to be in to talk about that because he can talk about specific enforcement activity.

Mr. BEALES. We are actively looking for spyware cases. We have open investigations. We will pursue those. We have brought cases that have challenged the deceptive downloads of dialers that disconnect you and reconnect you. We've brought cases that are very much the same kind of practice of once you're in the door, you can't get out until you buy the program. We've brought the extortion kind of case of buy this product and I'll stop sending you the ads that—this product will stop the ads that we're sending you.

We've brought all those kinds of cases. We will continue to pursue those cases. The problem is not one of legal authority. It is developing and proving a case in Federal Court.

Ms. SCHAKOWSKY. It sounds like this is a problem that's escalating rather than shrinking as we go forward. So what is it that consumers ought to be expecting from both industry and from the regulatory agencies right now? And then, Mr. Schwartz, I'd like you to add why it is that this broad privacy legislation might add relief to consumers?

Mr. THOMPSON. I think step one, I think responsible industry needs to tell consumers what software they're putting on the system, how it works and giving consumers a choice of whether to have it or not to have it.

Ms. SCHAKOWSKY. How big a problem is responsible industry? Usually when we're dealing with the most insidious scams, we're dealing with irresponsible players here who have the intention of robbing people of their information, et cetera.

Mr. THOMPSON. And that's exactly the point. One of the things I would like to see done is that the good guys can all work on the same baseline to say this is what the behavior, standard behavior

is in the industry, so we can begin to say anything that's outside of that is really ripe for our picking.

Ms. SCHAKOWSKY. Are you planning then to establish some kind of rule that would set those boundaries and the parameters rather than simply relying on industry itself to come up with that?

Mr. THOMPSON. As you said in your comments, we are at the beginning stages of talking about that. The workshop was very helpful. And as I said in my statement, I want effective and timely responses. I think we will continue to work with industry to see that that happens, but this is one issue that I think is important to have the committee's continued involvement and review.

Ms. SCHAKOWSKY. Clearly, the Congress and the bipartisan way is interested in stepping into this. If you're saying we should not, then it seems to me you have to have a very clear time line to come back with and say this is our plan, this is what we expect from industry. We really haven't seen that.

I would like to particularly get Mr. Schwartz'—tell me how this broad privacy legislation would help?

Mr. SCHWARTZ. Let's take a step back and look at the broader picture of online privacy. If we pass a law that says when you download software and you focus on the privacy of downloaded software, rather than general software, so let's say we do get the real fair information practices built into a software law that has notice, choice of intent for consumers, ability to access and see what they are turning over to the companies, etcetera. Then simply the bad acting companies simply start doing that from a server that's—where information is not downloaded to the computer, from somewhere remote. We've seen cases like that similar to that today.

By trying to define software and come up with privacy rules just for software, you're leaving out the exact same practices that we consider to be bad practices that are just done from a remote server.

Similarly, we saw this in web privacy as well. Early on we did not have any notices at all. As practices start to improve in one area, the bad acting companies shift and go to another area where they feel they can take advantage of consumers and that's going to continue to happen because that's the nature of technology. We're going to come up with new technological challenges. But if we have a broad law that focuses on the practice, rather than the technology, we can go after the actual root cause which is that companies are misusing people's personal information, not telling them what they're doing with it and keeping it in incorrect ways where consumers don't even know it could be used against them and they don't even have the ability to change it if it's wrong.

Ms. SCHAKOWSKY. Thank you.

Mr. STEARNS. The full chairman of the committee, the gentleman from Texas, Mr. Barton.

Chairman BARTON. Thank you, Mr. Chairman. I am reading from the FTC testimony here, the Commissioner's testimony, page 5, it says "at the workshop, FTC and Department of Justice staff members noted that many of the more egregious spyware practices described at the workshop may be subject to attack under existing Federal and State laws."

Later on in that same page it says, "However, investigating and prosecuting acts and practices related to spyware, particularly the more pernicious programs pose substantial law enforcement challenges."

Now then, my understanding, Commissioner, is that you said that you didn't think additional Federal legislation was necessary, yet in your testimony you're talking about it says "it may be subject to attack and pose substantial law enforcement challenges."

Why in the heck don't you support us legislating so we make it perfectly clear? If somebody walks in my house without my knowledge, without my permission, they're trespassing and there's a law that says that's illegal. And what you're saying is if somebody comes into my personal computer in my house, it may violate a law and it may be a problem, but it might be difficult to prosecute. Why not work with this committee to come up with legislation that makes it perfectly clear that it's illegal? And then if somebody wants that crap on their computer, they can opt to let it be.

I mean I don't understand. I really don't understand why we're having a semantical debate about something that everybody I've talked to is totally outraged about. I'm the moderate on this issue, by the way, on the panel.

Mr. THOMPSON. Well, Mr. Chairman, you know what I think about privacy in general, and we've discussed that before. I think that targeted legislation here at this time would be very difficult, if not impossible to define. And what I'm concerned about is leading people to believe that defining a certain kind of software, for example, will address the problem.

Let me give you an example. There are so many things in this area that would be a problem notwithstanding whether they informed you of it or not. If someone came in and told you we're going to disclose to you that we're putting software on your machine that's going to monitor your activity, that we can send to identity thieves, that would be unlawful no matter what. And it doesn't really matter——

Chairman BARTON. My understanding is there's not been one enforcement action even attempted. Is that true or not true?

Mr. THOMPSON. That's not true.

Chairman BARTON. That's not true. So you've done one?

Mr. THOMPSON. There are some things that are pending that I can talk about——

Chairman BARTON. Ah, some things that are pending. Maybe two, three? We've got 140 million people and I've yet to see a person when they find out this is on their computer says oh, that's okay. I'm okay with it.

Mr. BEALES. We have brought a number of cases, at least three or four, that challenged deceptive downloading of dialer programs that disconnect you and reconnect you to different service provider.

Chairman BARTON. Have you got any convictions?

Mr. BEALES. Yes, we have.

Chairman BARTON. You've got how many?

Mr. BEALES. In all of those cases. In none of those cases that have been fully litigated or resolved and none of our cases have we lost.

Chairman BARTON. If we were to pass a law that said you can't put anything on a person's personal computer without their explicit knowledge and if you do, it's a Federal crime subject to whatever the penalties are, would that help or hurt prosecute these cases, if we made it explicit?

Mr. BEALES. I don't think it would make any difference in the ability to prosecute these cases. It would make the process of installing new software with hundreds of different subprograms that I have no clue what they do, extremely tedious and difficult.

Chairman BARTON. And that's a good thing.

Mr. BEALES. No, it's not.

Chairman BARTON. You want this stuff on your computer? You're the only person in the country that wants spyware on your computer.

Mr. BEALES. No, I want my word processing program to work.

Chairman BARTON. We do too.

Mr. BEALES. And if you pass a law that says I have to go through each component of that word processing program as it installs and agree to that component, either I'm going to agree to everything and the spyware is still going to be there because I've been trained to agree to everything or my word processor——

Chairman BARTON. So now you're saying that spyware is necessary to install a program on your computer?

Mr. BEALES. No, I'm saying that software includes a lot of different programs where I don't know and I don't want to know exactly how they function to put a footnote in my document.

Chairman BARTON. And that's what spyware does?

Mr. BEALES. No, it's what software does.

Chairman BARTON. We're not opposed to software.

Mr. BEALES. But if you require consent to the installation of each program, then I'm going to have to go through each one of those programs——

Chairman BARTON. Let me just clue you. Unless I'm totally mistaken, when we get ready to move this bill all but a handful of the members of this committee on a bipartisan are going to be supportive of it. Now I'm not a software expert. I'm not a computer expert, but I can count votes on my committee. And I would encourage the Federal officials at the table to work with us on how to clarify the language that helps you enforce the law. Instead of trying to defend something that is not defendable.

I bet you that we could go to every person in this room that has a personal computer and I would be stunned unless they just cleaned their programs, cleaned their computers, they don't have spyware on their personal programs right now, including the people at the witness table. Every one of you.

And then I would double down and bet that if we asked if they wanted to take it off, almost everybody would say they want to take it off, except for you, sir, who apparently thinks it's a great thing which is what makes America great that we can agree to disagree, I guess.

Mr. BEALES. I think it is very difficult to draw a line around the what is the spyware, where I don't want it either and where we think there clearly are bad practices.

Chairman BARTON. Well, then work with us——

Mr. BEALES. We are happy to do that.

Chairman BARTON. Work with us to define the line.

Mr. BEALES. We are happy to do that to try to draw the line as well as possible. What is not clear to us is whether there is a meaningful line that can be drawn.

Chairman BARTON. I am very confident that with the lawyers we have on the committee and the lawyers that we have at your agency, we can draw the line.

With that, Mr. Chairman, I yield back the negative balance of my time.

Mr. STEARNS. That's all right, Mr. Chairman, I just want to buttress your argument by pointing out, as I point out in 2003 there were 2 million spyware software programs. Today, in the year—they project 14 million currently. So I would say to the Commissioner, with those statistics it sort of shows that the chairman is talking about a serious problem.

Mr. Strickland.

Mr. STRICKLAND. Thank you, Mr. Chairman. We've been talking about for lack of a better way to put it, bad actors, using spyware. Are there good actors who use spyware?

Mr. BEALES. Well, it depends on how you define it, but on many definitions, yes, there are. Keystroke loggers, for example, which can be used to steal personal information and for identity theft are frequently downloaded by help desks to try to figure out what it is you're doing, how it is they can help you use your computer better. That's a perfectly legitimate use of exactly the same software.

Mr. STRICKLAND. Is that done with the permission of the person whose information is being collected?

Mr. BEALES. Certainly with the implicit permission, whether it's explicit or not, I don't know, but certainly with the implicit permission because they've called and asked for help.

Mr. STRICKLAND. Let me ask this question. How many of you would agree with this statement, instead of regulating and outlawing certain types of software, we need to rather regulate certain types of behavior?

Do any of you agree or disagree with that?

Mr. BEALES. I would agree with that completely.

Mr. THOMPSON. I would agree with that as well.

Mr. STRICKLAND. And is it your impression that the legislation under consideration from my colleague from California an attempt to regulate software rather than an attempt to regulate behavior as you understand the proposal?

Mr. BAKER. No sir, if I may, I don't think that it's an attempt to regulate software. I think it does regulate behavior because it's not saying that any specific type of software is banned, but rather that software can't be downloaded to a user without their consent, without clear notice, without a means to uninstall it. So I think that is addressing the behavior.

And to your earlier question, I mean no, and I think this is what Mr. Beales was trying to describe earlier. We don't want a world where every time a consumer tries to use any program every web page they go to, every click of the mouse they're going to get a nothing dialog box saying do you agree, do you agree, do you agree? Nobody wants that.

But I think what we're doing here is establishing when things are loaded onto users' computers without their permission, from somebody that they have not agreed to. Certainly, if it's an update to their Microsoft operating system, to their EarthLink internet access, I mean that's something that the user has already agreed to and I think there's a fundamental difference there.

And I think that the statute does a pretty good job of distinguishing between legitimate and illegitimate users of software that's downloaded to a computer without the user's knowledge.

Mr. STRICKLAND. I have some problem understanding the difference between my Chairman's position and what I'm hearing from some of you in terms of if there's a problem and people are being abused in ways that they don't choose to have their computer used and is it possible to achieve what Mr. Barton wants to achieve and at the same time avoid the problem that Mr. Beales, I think, is trying to describe for us? Is there a way to accomplish both?

Mr. FRIEDBERG. I think as Congresswoman Bono mentioned, the devil is in the details and I think we all really want these bad actors to go away and for us to take back control of our computers. Everybody wants that. And we know that one element of the solution is kind of focusing on behavior, but when we write the clauses and the rules, we need to still tie it down to something. That's where the challenge is is tying it to the stuff, the software.

Mr. STRICKLAND. But do you feel that that can be accomplished without interfering——

Mr. FRIEDBERG. It is very, very hard. I have been thinking about this a lot and I am a computer scientist by trade and so I can tell you how hard it is. There are a couple of areas in particular that are very challenging. Uninstall requirements is one. The way you do consent is another. I know as a best practice I suggest to people in our company to do just in time consent and that's this concept of waiting until the most relevant moment when the user actually has some context to make a decision. If we put in certain rules and I'm not saying any particular legislation does this, but that require everything that happened in install time or transmission time, we've really missed the boat in terms of what, how users make trust decision. And we need to think about what's going to make my mom make good decisions when she's presented with the software and at what point does it make sense to have that?

I know in Windows, when something crashes, we pop up this window's error report. And we do that at the time of the crash and we tell the user hey, we might be able to find a fix for you if you let us send some data back to Microsoft to figure it out. So the user has great context. They know exactly hey, I want to keep going, I want my word thing to word and it's okay, I'm going to send this data and you can actually look to see what data is going to be sent, so you can understand your privacy impact at the time of the situation.

If we ask this question at the beginning, at installation time, there's no context. So there's all these different paradigms to consider, different ways to do consent, different ways to get this notice to show up.

Another is the user interface issues and design. As people pointed out, nobody wants to have 100 of these popups just show up and

completely color your experience. It doesn't make any sense. Also, we have new devices that are coming out almost every day and so it's very hard to figure out what their requirements are going to be. For example, there's this media center edition that we offer that's a 10 foot experience. Letters are really big. We only get two lines of text to communicate to the user these big issues, so we can't have very elaborate notices in that experience and likewise, if I have a watch that's really smart and it wants to download some new software, I've got very little room to provide that same notice. So we have to really think hard about all of these different scenarios. And that's why people are saying it's a little early. We really haven't had time to look at all of these, what I'll call test cases and watch out and figure out where the gotchas are. Because if we codify some of this stuff into law, suddenly we've tied our hands in an evasion which I think is a mistake.

Mr. SCHWARTZ. Can I address another issue along with some of the things that makes this more difficult——

Mr. STRICKLAND. My time is up, but——

Mr. STEARNS. Sure, why don't we just let them answer the question and call it quits.

Mr. SCHWARTZ. I was just going to say that the complexity of—this is not just like one company coming and monitoring the behavior of a computer user. These are—it's a complex network of affiliates, of individuals that are all involved in passing information to each other and cram the software down on computer users.

In the case that we brought to the FTC that we hope that there will be action on we found at least four or five different parties, two of whom didn't know what was going on at all. They were simply kind of pawns in the whole scheme, whereas two others, to our mind, seemed to be active actors trying to put spyware on people's computers and trying to get them to guy software that they didn't really need.

And in developing this case, it took us 2 months to put together and to turn it over to the FTC. It takes a lot of resources to put together these cases and track back the entire network. I think that's true for spam cases as well. Personally, I think we need to see the FTC get more resources to be able to go after these kinds of cases. Even if we had a new law that got at, closed up some of the existing holes, we would still have to have this same problem of being able to track down the bad guys.

Mr. STEARNS. Thank you and the author of the bill, the gentlelady from California, Ms. Bono.

Ms. BONO. Thank you, Mr. Chairman. It sure is nice to have again your full weight and that of Chairman Barton's behind this legislation and since we've started this hearing I think I've gained three co-sponsors, so I appreciate my colleagues paying attention.

But I am stymied by a lot of what I'm hearing and I'm also encouraged by a lot. First of all, we keep talking about prosection, prosecution. What the FTC has certainly failed to do is stop the proliferation of spyware and adware. You have failed in that. And it has grown exponentially and that is my intent. First of all, is to stop this growth, boom in this business, but also this bill is really about consumer empowerment. And as I mentioned to Mr. Friedberg, the devil is in the details in all of the legislation we

write here and I look forward to working with all of you in industry and my colleagues on crafting the perfect legislation. I have been revising it day by day, just to address these issues.

But you know, if we take this away from the realm of ones and zeros and change it to durable goods—for example, a car. I think Chairman Barton talked about this a little bit in trespassing. If I just bought a new car and I drove it home, parked it in my garage, would that give the automobile manufacturer the opportunity to come to my house and come into my garage and fix something because there was a recall notice on it without my knowledge? I don't think so. I do agree that there are beneficial uses of spyware, but I think if you warn the consumer first that this is all we're installing, it should be so simple. I love how Congress sometimes loses—I don't know that Congress has, but I think some people have, lost common sense. What is wrong with consumers simply knowing this is being installed. For example, Kazaa. I have two teenagers at home. They installed Kazaa. They thought this was great software. They were getting all of this free music, until I had to remind them about copyright and all of these things. I said—I had to point out to them somebody is still making money off of this and let me tell you how it works. And that's the way this all began. Somebody is making money. But it's not a songwriter. It's not a copyright holder. It's a third party you don't even know about.

My question to you, Commissioner, is would you allow that? Would you allow—let's say I've taken that new car, that new Ford I bought and it's no longer in my garage. I've parked it on the street, because it's a public highway, similar to the internet. So now I'm going to allow Ford to come by and fix that recall notice without my—and this is a legitimate use of spyware. I'm actually talking about a legitimate use because I believe that Microsoft and Symantec and legitimate software companies do warn you and they do say we're going to update your software and occasionally they allow you to hit a button that says yes, I know you're doing it. Sometimes it happens automatically. That's a convenience. I know it's happening. But would you allow that to happen to a Ford? Because that's what I'm hearing you say right now, it's okay. It's okay or maybe you'll enforce it or maybe you'll stop it, but right now it's okay.

Mr. THOMPSON. Let make something perhaps a little clearer. The challenge is the definition, because the same kinds of behavior—the same kinds of software can be used for beneficial and non-beneficial uses——

Ms. BONO. Excuse me, Mr. Commissioner, I disagree. I disagree. And you know, first of all, again as I've said, the beneficial use, most companies do inform you that they're going to be collecting data from your computer and they let you know that when you install the software. So that could be covered. We could allow that. The end user license agreement which is pages long, if we simplified to a simple box that would be covered, legitimate software sites could be covered. So I don't even know that you need to differentiate between because they are covered because they are doing that currently.

Mr. THOMPSON. What I'm concerned about is if you define something that is really based on consent and not in more detail about

behavior, then the very same thing that people are asked to consent to without any context can be used by that same company in ways that consumers don't want.

Ms. BONO. Which leads me, if I can jump because time flies.

Mr. Friedberg, can you tell me really fast, according to PestPatrol, there's something called Alexa and Alexa is a new tool bar and apparently it's bundled with Microsoft's Internet Explorer and I understand it collects information from websites that are visited. Can you briefly describe Microsoft's relationship with Alexa?

Mr. FRIEDBERG. There are two different versions of Alexa that I know of. One is a tool bar that Alexa offers that's not directly coupled to IE. There's another lighter weight version that's actually in IE that provides something called show related links. The lightweight version that's actually in IE sends an URL to the service and it returns back links that are similar to that link that you might be interested.

It's my understanding that that service does not retain or store any data and that the only information that's passed is this URL and it's sent back to the user. I can't speak for what the Alexa tool bar does. You'd have to talk to them and look at their privacy statement and read it very carefully, but again, when you look at the spyware results, when people say something is something on those lists, you have to look very carefully what the criteria is to understand which version of the software they're actually ranking. Just to be clear.

Ms. BONO. I look forward to working with you more on it and I know, Mr. Chairman, my time has expired. Thank you very much.

Mr. STEARNS. I thank the gentlelady. The gentleman from Arizona.

Mr. SHADEGG. Thank you, Mr. Chairman, I didn't know my time was up. I thought we had to go to the other side.

Gentlemen, let me begin with the gentlemen from the FTC. Commissioner Thompson, you said no legislation is needed and you said the FTC Act allows the Commission to take action against deception now.

Mr. Beales, you said we have the necessary tools to stop or at least address the practice. So both of you contend we don't need legislation.

I want to know how many people you have brought enforcement actions against and achieved a penalty against to date?

Mr. BEALES. Well——

Mr. SHADEGG. My time is very limited, just——

Mr. BEALES. It depends exactly what you mean by spyware. There are probably—this is a guess and I'll get you for the record precisely. There are probably 15 or 20 defendants that have been involved in the dialer programs, all of whom have been, all of whom have been penalized in one way or the other.

Mr. SHADEGG. I would like you to supply to the committee precisely how many you have gone after that you contend could be considered spyware and taken action against. Then I want to know first, right now, what are the potential penalties you can impose?

Mr. BEALES. We can get full redress for whatever money they have made from consumers and——

Mr. SHADEGG. Full redress. Can you impose criminal penalties?

Mr. BEALES. No, we have no criminal authority.

Mr. SHADEGG. So full redress means they make $200,000 out of the deal, they steal that from me, you can get back the $200,000. What's the disincentive if all you can get back is what they took from me, what's the disincentive for them to do that again?

Mr. BEALES. Well, in a typical case, there's not anything like $200,000 left. And——

Mr. SHADEGG. I've worked very extensively on identity theft legislation and I guarantee you when your identity gets stolen, it's nearly impossible to quantify the damages people suffer and calculating how much they've suffered is near impossible. The point is in all of criminal law, and I used to work for the Arizona Attorney General's Office, if all you can get back from the bank robber is what he took, there's no disincentive to rob the bank. So I guess my question is do you have the ability to impose penalties beyond what you think they've profited?

Mr. BEALES. We do not in the typical case of unfair and deceptive practices. Many of the kinds of conduct at issue here may violate other criminal laws. It's common——

Mr. SHADEGG. Then I want to know if those criminal cases have been brought. I want to know all of the cases you've brought, all of the penalties you've exacted and then I want to know all of the criminal cases that have been brought that you're aware of against people that engage in this conduct. And I'd like you to supply that to the committee.

Is that all right?

Mr. BEALES. We will be happy to do our best.

Mr. SHADEGG. Let me move to a separate topic. One of the concerns I have is that in many of these agreements that we talk about you say well, they're legitimate things that are being done. There are also illegitimate things that are being done.

What are you doing with regard to what I call fine print permission, that is, I sign an agreement with one of the legitimate companies and buried deep, deep, deep in the fine print is a very, very small disclosure that says I give you permission to get into my computer and do all kinds of things that no rational person would want to do.

Are you pursuing that now?

Mr. BEALES. We think disclosures need to be clear and conspicuous. What that means depends on the consequences of the particular disclosure.

Mr. SHADEGG. Have you ever looked at the disclosures that are required? Have you brought an enforcement action against somebody?

Mr. BEALES. We've brought many actions involving disclosures that were not sufficiently clear and conspicuous.

Mr. SHADEGG. Okay, I'd like you to supply me with a list of those that relate to abuses of, for example, getting into my computer and taking privacy information that I don't approve of.

Mr. BEALES. I don't think we've brought cases that involved end user license agreements. We've brought numerous cases that involve insufficiently clear disclosures in a wide variety of contexts and the legal principles——

Mr. SHADEGG. But not for as an individual consumer?

Mr. BEALES. I'm sorry?

Mr. SHADEGG. You said not end user license agreements. I think we're talking about end user license agreements right now, aren't we?

It's my computer they're getting into and some would contend with permission because I signed agreement that had a fine print disclosure.

Mr. BEALES. We have brought numerous cases like that, not in the software context. The disclosure issue though of is it clear and conspicuous is not fundamentally different.

Mr. SHADEGG. Except we're talking about the software context and if you haven't brought any of the software context, that doesn't sound like that's an enforcement tool that will help solve those problems.

I'm going to run out of time. I want to move on, so I'd like to know what you contend fits there.

You have said that it would be impossible, Commissioner, to define this issue. I want you to tell me under what circumstances it would ever be appropriate for someone to get into my computer without my permission and monitor every single keystroke of my computer forever and give that information away to somebody else?

I mean that's one of the most offensive practices that I think is going on here is they get into my computer. You talked about it. They put a stroke monitor on my computer and they know everything I do on that computer and then they sell that information or use that information.

My question to you is, you say it's impossible to define this legislation. Under what circumstances would anyone ever want to have it occur that someone can get into my computer or your computer, monitor every stroke I make without my permission and give that information away or use it for their benefit, every stroke?

Mr. THOMPSON. I can't answer that question because I know that it would bother me and I know that one of the problems with the legislation that's proposed, to the extent to ask you to give permission for context, out of context, you may—what I'm worried about is consumers are going to be asked to say yes to behaviors they don't even know are going to happen.

Mr. SHADEGG. You just admitted to me that there is never, you can't imagine—and this is your business—you can't imagine a circumstance under which it would ever be appropriate for somebody to get into someone's computer without their permission and monitor every single stroke——

Mr. THOMPSON. For all circumstances——

Mr. SHADEGG. For ever. I understand that when I go into my Bank One account, I have the choice on my computer to say I want to permanently register both my user ID and my password. That's a single transaction. What's going on here is they're in my computer and they do that forever. I quite frankly, and I'm running out of time, I do not see a thing different between that and wiretapping. And we don't say to people who have telephones, you know there's a danger that someone might tap your telephone and listen to all of your phone conversations, so you should buy a device, we should teach you that, we should address this as consumer education, we should teach you that that might happen and then you

should buy a device to put on your telephone that stops them from tapping your telephone. And yet what I hear both of you from the FTC saying is that even though someone under spyware can get into your computer, Congressman, and can without your permission put a stroke recorder I think was the term you put on it and record every stroke you make and every stroke your kids make and every stroke your wife makes and know every where you go and everything you do, we think the way to stop that is to tell you, Congressman, is to be aware that it might happen and to make you go buy something to put on your computer to stop it.

Mr. BEALES. Congressman, I think what we're more worried about is the perfectly legitimate download that you agree to of that keystroke monitor from the help desk——

Mr. SHADEGG. No, no, no, no. I never——

Mr. BEALES. That's buried in the fine print that gives them permission to do that indefinitely.

Mr. SHADEGG. I got a flash, I would never ever, ever agree to give permission to someone to monitor every single keystroke of my computer for ever and ever, for a week, for a month. I might give permission for one transaction. I might give it to my bank for two transactions. But that's not the abuse we're talking about and you said it's impossible to write legislation defining this problem and yet the Commissioner just admitted to me that he can't imagine ever a circumstance in which it would be appropriate.

Quite frankly, it's simply identical to my having my telephone tapped—I would never give somebody permission to tap my telephone.

Mr. BEALES. Congressman, I think it's more akin to having an extension on your phone where sometimes somebody picks it up and——

Mr. SHADEGG. In my own house? These people aren't in my household. These people are somewhere else, they're miles away and they're doing this without my permission.

Mr. BEALES. And you invited them in to help you with your transaction.

Mr. SHADEGG. Exactly, as if I called the car dealer. If I call the car dealer and said I'm interested in a car, I wouldn't have said to that car dealer, oh, by the way, because I called you you have the right to tap my phone for the rest of history.

Mr. BEALES. I agree. If that was in the consent, I wouldn't think it was adequate, but that's because it's not a consent problem, it's a behavior problem.

Chairman BARTON. Will the gentleman yield?

Mr. SHADEGG. I think it is a consent problem and I think the last point here that I want to make is——

Chairman BARTON. I would ask unanimous consent that Mr. Shadegg have an additional 2 minutes.

Mr. STEARNS. Unanimous consent, so ordered. I would point out to the chairman we're going to have a second round here, so I would encourage the gentleman from Arizona to stay around.

Mr. SHADEGG. Unfortunately, I can't stay around, but I'd be happy to yield.

Chairman BARTON. If I have a problem with my telephone, I call Southwestern Bell and I say there's something wrong with my

phone line. And Southwestern Bell sends a repairman to my house to check the phone lines and hopefully repair it, but the Southwestern Bell repairman doesn't just move in with me.

He doesn't say what's for supper and what are you going to be watching on TV and you know. Put a beeper on me so that wherever I go make sure that I'm home in time to cook and clean for him.

So I just simply don't understand why we can't agree that these unwanted intrusions should be totally explicitly illegal. We're not talking about asking Microsoft when I buy the computer, we have to sign an agreement to use the Microsoft operating system on the computer. We're not talking about that. We're talking about programs that get put on our computer without our knowledge and are doing things that we don't want to be done and taking information that we don't want to be taken.

Do you all agree with that?

Mr. BEALES. I do. I think it's a question of whether you try to prohibit that and make it illegal under the general approach of the deceptive practices that were used to install it, or whether you try to write legislation that draws bright lines and says you have to do it exactly this way.

We agree there's a problem. We agree that the kinds of conduct you're talking about here are illegal. The question is what's the best kind of a statute to address that. Is it the general deceptive practices authority we've already got or is it something more specific that says go through these hoops and that constitutes consent to this keystroke logger that lives there forever.

Mr. SHADEGG. Let me just tell you where I see you're coming from from my perspective. You're telling us—and I'm a former prosecutor with the Attorney General's Office in Arizona. You're saying current law is adequate to handle this problem. Oh but, we're really not enforcing the law right now. We think you can't define the issue, although I just gave you a definition that neither one of you could say you're right, Congressman, that ought to happen some time. And then your last answer is self-regulation. I am typically a guy who believes very much in industry self-regulation. But Commissioner Thompson, you pointed out that we've got criminals out here engaged in this activity that don't care that it's already illegal. You tell me how the legitimate industries are going to stop those criminals with self-regulation. It's not going to happen.

We've got a wide open door for criminals here. Your answer is well, give us time, we may bring an action later. I'm sorry, I just don't think—of course, it's difficult to write a law in any area. We understand that writing definitions in this kind of complex area of any law is very difficult and we don't want overly broad legislation, but I've got to tell you, doing nothing about the fact that somebody can get into my computer and record every single stroke on it and that I ought to try to self-protect against that which to me is wiretapping of the current generation, just makes no sense.

I applaud Ms. Bono and yield back my time.

Mr. STEARNS. The gentleman's time has expired. My unanimous consent, we have a guest who is not a member of the full committee or the subcommittee, obviously. We're going to allow an op-

portunity for him to ask questions for 3 minutes and then we'll have a second round for anybody who would like to—just for the members, we'll have an opportunity for a second round and Mr. Inslee will be offered one opportunity for 3 minutes. So I recognize the gentleman from Washington.

Mr. INSLEE. Thank you, Mr. Chairman. First I want to thank Mary Bono for her vision on this to understand that action was needed by Congress and she's been ahead of the curve and I look forward to working with her and others on this. I want to thank the committee chair for allowing me to participate and the reason is that I'll be introducing an alternative, a bill to try to address this very difficult issue. And I believe it is clear that we need to act and I'm disappointed that the Commission has allowed the difficulty of this task to overwhelm the obvious necessity for action here because we do need action.

The bill I will be introducing will have two approaches and I think it's a pleasure to hear the testimony of the witnesses because it sounds like we might be on the right track. No. 1, the bill I will be introducing will address behavior, rather than just a designation of type of software and I've heard sort of unanimity of the panel to date, suggesting that that's a model that will allow us to cut with a sharp scalpel, rather than a blunt instrument and that's what we need to do in this highly tech area.

Second, it will try to have just in time notice and consent because in thinking through this, to me, having the consumer have the ability to do notice and consent at the time of the execution rather than just even a transmission will be a preferable way to do this. So that's the two thrusts and I look forward to working with the committee members on that.

I want to just give the Commission a moment, my take on what is going on is the reason there has been such a spectacular failure by the American government to protect consumers from this outright abuse of their privacy that is going on in hundreds of thousands of cases today is that we have a 20th century law trying to regulate a 21st century type of new technology. And what I hear from the Commission today is kind of like if in the wild West if the bunch rode in and robbed the bank, the regulators are trying to say that the townspeople would say well, let's call for self-regulation. I don't think that's what the townspeople are calling for here. They're calling for a strong sheriff and a clear definition of what is allowable and now allowable.

Now isn't it true that the reason that you haven't taken much enforcement action despite these hundreds of thousands of privacy violations is that there is relatively great ambiguity and vagueness that makes prosecution very difficult for you right now because we have so much vagueness in existing law?

Mr. BEALES. No.

Mr. INSLEE. Then what is the reason?

Mr. BEALES. The reason—what limits our ability to bring these cases is that, and your bank robbery analogy is somewhat apt, is the bad guys ride off into the hills. But these are cyberhills and there are no footprints.

Mr. INSLEE. Well, that just won't wash. In today's technological society so that that we have hundreds of thousands of violations

and you can't find a half dozen violators, that doesn't wash. You need to hire some people that come out of private enterprise, if you can't find these guys.

My time is limited, I need to ask another question. There was discussion about notice and consent and we'll get to that next round, if you will allow, Mr. Chair.

Mr. STEARNS. Well, I was just hoping you will participate and I give you that opportunity, but I'll start with myself with the second round of questions and I thank the gentleman.

We have the chairman of the Oversight and Investigations Subcommittee and I am very pleased to see him arrive. Before I start, Mr. Greenwood, congratulations and we welcome you here. If you want to have some questions, you're welcome.

Mr. GREENWOOD. I do. Good morning, gentlemen. I apologize for missing the hearing heretofore, but it couldn't be helped.

On my home computer, I have experienced what my staff tells me is called browser hijacking. And that is we have a home page that we had set up that's useful to our family and all of a sudden this bizarre home page is there and it won't go away. I keep going back and re-establishing, resetting MSN, I think it is, is our home page and this thing pops up and it's annoying in a lot of ways, but one of the ways it's annoying is if you try to use it as a search engine, it only goes—it doesn't take you where you want to go. It only goes to commercial sites that are trying to sell you something.

And my staff fellow who is with me this morning said that he just checked his computer and he has 81 spyware programs that have been stuck into his computer. So the question is first off, can anyone define for me, browser hijacking just so I know we're on the same page. And then has the question—has the FTC taken any actions? I believe there's been a complaint filed by CDT against MailWiper and also against Seismic Entertainment Productions. Has the FTC taken any action with regard to browser hijacking? If so, what is that? And under current laws, would browser hijacking be actionable and does the FTC have additional authority to pursue those actions?

There are all the questions and I'd be happy to hear from any of you that would like to comment on any of those questions.

Mr. FRIEDBERG. I'll just start by defining browser hijacking for you. It's the changing of the key settings in the browser, specifically the home page or the search page without appropriate notice and choice to the user.

Mr. GREENWOOD. I'm sorry, I was interrupted. Say that again?

Mr. FRIEDBERG. It's the changing of the key settings in the browser, specifically the home page and the search page are most common without appropriate notice and choice where you aren't told and you can't undue it.

Mr. GREENWOOD. Is it illegal?

Mr. BEALES. Yes, it is. We have brought cases that challenged the practice of page-jacking which is essentially the same thing. You try to go to one page and you end up on another. We've challenged that as an unfair practice and have been successful in doing that.

Mr. GREENWOOD. You have been successful. And what consequences have people who have successfully been prosecuted faced?

Mr. BEALES. That particular case was one that was brought in about 2000, I believe, and I don't know exactly what the sanctions were in that particular case.

In general, we can get full redress for consumers who have been injured. We get a permanent injunction——

Mr. GREENWOOD. What would be—how do you redress me? How do you—my wife has been trying for years, but how do you compensate me fairly for this experience?

Mr. BEALES. Well, in cases where injury is difficult to assess and this is certainly one, we would frequently go on a disgorgement theory of getting back all the money that whoever was behind this had received.

Mr. GREENWOOD. It's obviously continuing to be done with impunity, the people who do this must not have—they obviously don't think they'll ever be caught or if they think that if they do, they'll make enough money that it will be well worth their effort.

What do we do about that?

Mr. BEALES. We are trying very hard to make sure they're wrong on both counts.

Mr. GREENWOOD. So what should a consumer do? What should I do in this case? What are my options as a consumer to respond to identify the printout, the home page, the uninvited home page and send it to the FTC or what?

Mr. BEALES. As a way to complain, yes. We would love to hear from consumers about specific complaints. That's very useful to us as the starting point of an investigation.

Mr. GREENWOOD. What's the most difficult—obviously, anyone watching this hearing anywhere in the country right now, I imagine a very significant portion of them, that's exactly what happens to me and they could all make complaints to the FTC. What's your resources limitations have to do with how much action would actually occur?

Mr. BEALES. What we use our complaints for and if anybody is watching, complaints can go to www.ftc.gov. What we use our complaints for is to identify targets for law enforcement based on the volume of complaints. We do not have the capability to resolve individual complaints, but it does help to figure out what kinds of practices are out there, who is doing them and then target our enforcement actions against those cases.

Mr. GREENWOOD. My time is up, but do plaintiff's attorneys file Class Action suits in these cases with any success?

Mr. BEALES. I don't know of any in these cases. The problem that we have in terms of financial relief for consumers is that there's not money and that tends to make them unattractive cases for plaintiff's attorneys as well.

Mr. SCHWARTZ. In the MailWiper case that you mentioned that we brought to the FTC's attention, there is a class that's bringing a case in North Dakota right now against the same companies that we filed the complaint against.

Mr. GREENWOOD. Thank you, Mr. Chairman.

Mr. STEARNS. I thank my colleague and I thank him for taking the time to come out.

I'll start the second round of questioning. Do any of you know about the law that passed in the State of Utah?

Mr. Baker, as I understand, this law allows a private right of action, so what Mr. Greenwood is talking about or Mr. Shadegg is talking about, I think they have a private right of action.

Mr. Schwartz, is that correct?

Mr. SCHWARTZ. No, you would need to be a website owner or a trademark holder. So unless Mr. Greenwood runs his own website out of his house, he would not be able to sue in the private right of action under the Utah bill, Utah law.

Mr. STEARNS. Well, I mean I'm trying to get to the point that Mr. Greenwood and Mr. Shadegg touched on. What rights should consumers have in the courts when this occurs?

Mr. Baker?

Mr. BAKER. Speaking to the Utah law specifically, Mr. Chairman?

Mr. STEARNS. Yes.

Mr. BAKER. There's great concern among the industry, many, many companies that the Utah law is overbroad.

Mr. STEARNS. Overbroad. Because it allows too much possibility of litigation?

Mr. BAKER. Not so much that is that it outlaws too many things and there's great concern that, for instance, a library's attempt to install filtering software to keep children and other patrons free from pornographic websites or parental controls even, that those—that this wall would, in fact, bar applications such as that. I don't think that that's what any of us would be after.

So getting back to the House bill, one of the things we like about the pending legislation here is in fact the pre-emption provisions because we are concerned. It would be a cruel irony if, in fact, you have an anti-spyware statute that is so broad that it might even bar the downloading of anti-spyware software.

Mr. STEARNS. Right, so I think it's important to say we see one State passed a law and we should understand what's good and what's bad about it, so that if we move forward on the Federal, that we not incorporate the bad and try to do what's good. And at the same time, do you think a Federal law should prevent private right of action?

Mr. BAKER. This is just a personal observation.

Mr. STEARNS. Yes.

Mr. BAKER. I'm always a little wary of private rights of actions in Federal legislation and this was one of the things that was debated in the recent Canned Spam Act, for instance. Ultimately did not—was not included, because you do run the risk there of otherwise legitimate companies facing the wrath of multiple lawsuits.

Mr. STEARNS. And Mr. Friedberg, how do you feel about that, do you agree with Mr. Baker in that respect?

Mr. FRIEDBERG. I really can't comment on private rights of action. That's not my expertise.

Mr. STEARNS. Okay, anyone else? Mr. Schwartz?

Mr. SCHWARTZ. We're usually in favor of private right of action in this type of case. It would depend on the definition though if it

is overly broad. We would have concerns about how that might be misused in the courts. But generally speaking, we would want to see private right of action in a privacy law that would move forward.

Second, the Attorneys General, as well, that's something in the Utah law that Attorney General, even the Attorney General in the State of Utah can't act. That seems to us to be a concern as well. We want to see the Attorneys General have some power as well.

Mr. STEARNS. I would just say in passing to the Commissioner, we passed the Spam Act which prevents all this spam material coming into the computer and then we passed the Do Not Call List which was saying we didn't want to have telemarketers come into our home. So if you follow the logic in both of these you're vigorously implementing, if we're trying to talk about e-mails and we're talking about telemarketing, it seems to me then the Federal Trade Commission would welcome some kind of Federal legislation to prevent spyware.

Does that seem logical?

Mr. THOMPSON. I understand your point. As was said earlier, the devil is in the details. The Canned Spam Act is an interesting piece of legislation. It's still a very significant challenge to get at the worst actors who are involved in spam for a number of different reasons, including the fact that most of the people who are the most egregious actors really don't care about the law. And that's where the real challenges rest.

Let me say this too. I don't want the Commission to be characterized as being uncaring or inactive——

Mr. STEARNS. No, I want to give you the last word here. Here's your chance.

Mr. THOMPSON. We brought the workshop to bring public attention to this issue. We're asking industry to self-regulate for one very important reason, we want them to begin to outline standards. That's going to be instructive for us on this issue going forward no matter what, not only on talking to consumers about what's good behavior and what's bad behavior, but even in talking to us as law enforcers or talking to legislators about understanding where that line is.

Right now, that discussion hasn't really taken place and that's one of the reasons why we've asked for the workshop to begin to outline the parameters of what this issue is about.

Mr. STEARNS. Thank you. My time is expired. The chairman of the full committee, the gentleman from Texas, Mr. Barton.

Chairman BARTON. Thank you. I want to ask Mr. Friedberg a question. Your responsibility at Windows is to monitor the privacy protection that is built into the base Windows program, is that right?

Mr. FRIEDBERG. Actually, the way I define my job is I would like to think that I make people feel better about using Windows by protecting their privacy, most notably by giving them notice and choice and appropriate control.

Chairman BARTON. Is it Microsoft's assumption that the computer in a person's home is that person's private property?

Mr. FRIEDBERG. Their physical hardware, yes, I believe they license the software from us.

Chairman BARTON. Is it Windows' position that access to that computer is the prerogative of the person who owns it in their home?

Mr. FRIEDBERG. A person should be able to control what goes on in their computer, sure.

I don't know,d id that answer your question?

Chairman BARTON. So if we wanted to postulate such a thing as computer trespass, just like if somebody walks through the physical front door of my home without my permission, they've created a crime. They've trespassed.

So if somebody comes into my computer without my permission and I chose to prosecute whoever came in to my computer, I could accuse of them criminal or computer trespass. Now I don't know that there is—I'm not an attorney and this isn't the Judiciary Committee, but the concept of computer trespass.

Mr. SCHWARTZ. I was just going to add that the Computer Fraud and Abuse Act is partially aimed at that idea. If there is damages, certain kinds of damages, the Department of Justice is supposed to be able to go after companies that do trespass-caused damage on people's computers. We haven't seen them act in these kind of cases though.

Chairman BARTON. We're kind of talking past each other. In my first round with Mr. Thompson, Commissioner Thompson and Director Beales, they were talking about deceptive trade practices. I don't consider it a deceptive trade practice when somebody violates my privacy. They've trespassed against me.

We all seem to be in agreement that if it was a live person coming into our home, that wouldn't be right unless we wanted them in our home. But when we talk about using the internet to come into our personal computers, then you get into this debate about if it's fair or unfair and all the good things that theoretically happen when people do come into our computers without us knowing about it.

Well, I can have a debate that all day, but I want to ask the gentleman from Windows if this concept of computer trespass is something that we can work with?

Mr. FRIEDBERG. From a personal perspective it makes intuitive sense to me. I very much believe in making sure there's consent before someone does something on your computer.

Chairman BARTON. Now I understand that the FTC doesn't have criminal prosecution ability. You're civil. You can fine people, but if we worked with the Judiciary Committee to define as a crime the concept of computer trespass, Commissioner Thompson, is that something that the FTC would be comfortable working with us to get the definition right?

Mr. THOMPSON. We are always happy to work with the committee. Let me just point out a challenge though. The trespass issue is an interesting issue. What I find more often the question is defining when you've actually invited people in and going further is when you've asked them to actually come into your kitchen because you may have asked them to come in to your house, but you may not have asked them to walk around to places where you didn't want them to walk around.

Chairman BARTON. I understand that. And I from time to time on my personal computer in Inez, Texas have downloaded Windows software and I have downloaded game, videogame software from certain companies and I wanted that. Now if they put something on my computer when I downloaded what I wanted that I didn't know about to track my behavior, I want to put a stop to that.

If I open my door and there's somebody from Amway outside the door wanting to sell me a product, I can make a decision and invite them in and buy the product or not buy the product. And even to this day and age, Inez, Texas is a small enough town that we do have some door to door salesmen and saleswomen still come by and I'm okay with that, so I want to apply that same concept of privacy, the physical front door, to the computer front door. And I want the Microsoft people to help us and I want the FTC people to help us and at a certain point in time, we want the Department of Justice to help us.

If you all understand that, then we're going to be okay. Nobody is trying to prevent a legitimate business entity from providing a product that is wanted to the end user in their home. We're all, I think, trying to prevent the unwanted intrusion that is used for purposes that we have not approved and most of the time without our even knowing about it. That's what we're trying to prevent.

Mr. FRIEDBERG. We are very eager to work with anyone who is trying to address this problem.

Chairman BARTON. With that, Mr. Chairman, I'm overextended again and I'm going to yield back.

Mr. STEARNS I thank the chairman.

Chairman BARTON. Let me say one final thing. I don't want anybody to be under the impression that this hearing is just a hearing and nothing is going to happen. We are going to move heaven and earth to work on a bipartisan basis to modify the Bono Bill and move it at subcommittee and at full committee and onto the floor and through the House and hopefully get a companion bill in the Senate and go to conference and get a conference report that's passed by the House and the Senate this year.

I'm not guaranteeing that that will happen, but that is the intent of this hearing to start the process, regular order to make that possible.

Mr. STEARNS. I thank the chairman. The gentlelady from California.

Ms. BONO. Thank you, Mr. Chairman, I kind of liked it up there in that big fancy chair, but I'm happy to be back here and to Chairman Barton, also you forgot the best part of due process and that was where the President signs the bill, ultimately, so I'm looking forward to that day as well.

Chairman Stearns has mentioned repeatedly, I believe, about what will become a patchwork of State laws and we've seen the Utah bill. There's also a pending bill in State legislature of California that was introduced in February. Now as I understand the language, and what it does, they say it prohibits a person or entity conducting business in California from hijacking a user's computer, from inhibiting the termination of a computer program and from surreptitious surveillance of a user's computer in California.

I don't know that that protects the California consumer, but I know that lends to the nightmare of patchwork of different State laws, so I think that further gives weight to what we're trying to do here.

I also want to point out that California was the first State to pass anti-spam legislation.

Commissioner Thompson, I understand you opposed anti-spam legislation on the Federal level. Is that true or did you support anti-spam legislation?

Mr. THOMPSON. I don't believe I expressed opinion one way or the other.

Ms. BONO. Okay, did the FTC oppose originally?

Mr. BEALES. The FTC at various points along the way did not recommend legislation.

Ms. BONO. Okay, and are you using it now?

Mr. BEALES. Well, when canned spam passed, it was with the Commission's support. We are announcing our first case is today.

Ms. BONO. Great news. Hopefully that will be the same case here, that we're going to turn you guys around too and we'll be one big happy family.

But on to Microsoft, you mentioned a problem with my bill and I wanted a one-step removal tool. As I understand it, with Kazaa or a real fun version of spyware, adware, I guess Bonzi Buddy. If you guys are parents, you know what I'm talking about, this cute little purple gorilla swings suddenly on your monitor, and kids love to download this little Bonzi Buddy. But to remove it is nearly impossible, and when we've tried to remove little Bonzi Buddy, the purple gorilla, he somehow comes back. Is it that impossible? Microsoft, with all of these programs, especially Windows XP, why can't we do one step removal tool?

Mr. FRIEDBERG. Well, actually, it largely due to the bad actor in this case. If they don't provide that kind of functionality when they install the software, it's going to be hard to figure out how to remove it.

I totally advocate the goal of trying to make things as easy for people to uninstall as possible. The only trick, again, the devil is in the details is that software is a complex kind of beast and there's scenarios where it's very hard, if not impossible, to remove parts of software without removing larger chunks of things. You can't remove things, for example, that are already in use by other programs and certain things that might be for security, you might want to think twice about removing.

Trying to get it right in codifying into law how an uninstall should work is what's the challenge, not the intent of having control over your system. Fully agree, we want to be able to get rid of stuff when we don't want it. At a minimum, disable it, neutralize it and at best actually not having any remnants left over. It's just kind of challenging to do it in all cases.

Ms. BONO. It's like those little .dll files, isn't it?

Mr. FRIEDBERG. The problem is legitimate software has reasonable scenarios where uninstall is just not that easier. It's the way software is.

Ms. BONO. Well, it seems to me that if this law were passed, that when people installed this onto computers, they would just have to

come up with a way to do it, and it's common sense to me if you instruct him to build a program that way that they could. If we don't tell them to do it, they're not going to do it. But is it your understanding to? Am I missing something on removing Bonzi Buddy and Kazaa? Are they sort of self-perpetuating?

Mr. FRIEDBERG. There's this other kind of problem and some people call them tickler applications and stuff like that. They'll actually attempt to reinstall a piece of software after you've deleted it. I consider this very deceptive practice since it's a covert install and hopefully there are laws already that sort of address this kind of behavior.

Ms. BONO. How is that different than a virus? I understand how it's different than a virus, but I'm hoping you'll answer the question the way I want you to answer it. A virus we all see as detrimental because it's self-replicating and it passes from computer to computer without knowledge. But suddenly now because somehow you've downloaded this thing and it's not self-replicating, just because it's passed on by a third party, in a sense it is a virus. I see it as a virus without the self-replicating tool, but it's just as harmful as a virus is.

Mr. FRIEDBERG. Along those lines, when you look at a virus, people talk about viruses because of how they propagate, as you point out. And it's the payload inside the virus that's the issue. I mean some viruses might be benign in terms of how they actually do what they do. They may just count things or something, who knows?

But it's what the payload is doing and if someone is doing something destructive on your machine, they should be punished, regardless of how it got there.

Ms. BONO. Thank you. Can you briefly define for the sake of refining my legislation two points, why a cookie is not considered spyware?

Mr. FRIEDBERG. A cookie is just a simple data storage facility. It makes life easier for people who may surf the web in order to keep state. It's not an active component and the way the web is set up, these cookies are only read by the websites that put them there. It's their local storage to make life easier for you.

It's up to them, the site that you're going to, to tell you what they're going to do with the cookie and you now, if they're going to track you or do some kind of behavior like that, it needs to be in their privacy statement. But cookies in themselves are not necessarily anything worse than a file.

Ms. BONO. Thank you. Also, are there any type of spyware functions that are utilized in good ways for the enabling of e-mail or instant massaging?

Mr. FRIEDBERG. I just think of spyware using that term as something that's a negative. I would never consider something spyware as being a positive thing. The functions of spyware may have positive elements. For example, tracking. I know I got to Amazon.com and I get suggestions for books I might want to read that are similar to other books and I like that. I call that personalization when the tracking is done with my consent. I have control over it and it's to my benefit. So tracking is not the problem. It's unauthorized tracking or covert tracking which is spying.

I can't imagine a time where that's valid, except for maybe some small examples, for example, as a parent, maybe you want to track the behaviors of your children and you want to have the right to be able to put some kind of key logger to be able to see what they're doing. If that's okay by local law, then that should be permitted. Likewise an employer/employee relationship. If it's allowed that you can monitor employee behavior, you're going to use one of these tools that we talked about and that's a valid, potentially legal use that makes sense.

Ms. BONO. Actually, the bill clearly defines those two uses as fine. But also, I always think that's sort of repetitious anyway because the owner of the computer is generally the parent, first of all. So you're installing it on your own property and I would think the same with an employer, but we do define those two in the bill.

Mr. Chairman, I have gone over my time. I just really want to thank you for this hearing and thank our panelists. I really look forward to passing something that protects the American consumer and continues to broaden the American experience with computers.

Mr. STEARNS. I thank the gentlelady and we'll conclude our hearing.

Mr. Friedberg, I think you answered her question when the question was it's not easy to take the spyware off your computer. If I went back to my computer without having a high tech person, I couldn't do it, could I?

Mr. FRIEDBERG. Actually, what I recommend to people nowadays is to use a third party and a spyware tool.

Mr. STEARNS. You need a spyware tool, you need a third party and somebody needs to have technical expertise.

Mr. FRIEDBERG. As of today.

Mr. STEARNS. As of today.

Mr. FRIEDBERG. That's the situation. These things are relatively new and people are just trying to catch up with the way that they're doing what they're doing.

We would like to see longer term solutions that are more holistic, especially in the technology area because we have some control over that, that make it less likely that this can happen to you.

Mr. STEARNS. But I think it goes to the heart of what Ms. Bono has mentioned is, in the heart of the discussion today is that the average consumer cannot take these off themselves and second, they don't even know they're on the computer.

Mr. FRIEDBERG. I can't take them off myself.

Mr. STEARNS. You can't.

Mr. FRIEDBERG. I use a third party tool at this point.

Mr. STEARNS. Okay.

Mr. FRIEDBERG. And I'm looking for relief as well.

Mr. STEARNS. I'll just conclude by saying that I think spyware is not just at our gates, but through the gate, through the door of our homes and now in our computers with full spying privileges and I think this hearing has brought a lot of information to the forefront and helps obviously all of us as legislators to think this through and try to come up with legislation which is balanced and I want to thank all of you for your time and your patience. With that, the subcommittee is adjourned.

[Whereupon, at 12:22 p.m., the hearing was concluded.]

[Additional materal submitted for the record follows:]

PREPARED STATEMENT OF ROGER THOMPSON, VICE PRESIDENT OF PRODUCT DEVELOPMENT, PESTPATROL, INC.

Mr. Chairman and Members of the Subcommittee, thank you for the opportunity to submit comments on the important issue of spyware and its threats to the security and privacy of consumers and businesses.

Before I offer an assessment of the situation and possible actions to address it, let me provide a brief overview of my company. PestPatrol was founded in May 2000 by a team of security software professionals to counter the growing threat of malicious non-viral software. We are the leading provider of anti-spyware software to consumers. Our database of malicious code—what we call "pests"—is the most extensive in the industry and serves as the basis for many of the research results about which we read in the press.

*Definition Debate*

No one debates that spyware is becoming a relentless onslaught from those seeking to capture and use private information for their own ends. However, there continues to be much debate about what constitutes spyware.

While that debate is an important one in terms of possible remedies, we can count the cost that unfettered spyware is having on individual users as well as on corporate networks. Regardless of whether we agree to divide the term spyware into various subsets such as adware or malware, the truth is that any software application, if it is downloaded unknowingly or unwittingly, and without full explanation, is unacceptable and unwelcome.

At PestPatrol we define spyware as any software that is intended to aid an unauthorized person or entity in causing a computer, without the knowledge of the computer's user or owner, to divulge private information. This definition applies to legitimate business as much as to malicious code writers and hackers who are taking advantage of spyware to break into users' PCs.

*Spyware Dangers Real and Extensive*

The dangers of spyware are not always known and are almost never obvious. Usually, you know when you have a virus or worm—these problems are "in your face". Spyware silently installs itself on a PC, where it might start to take any number of different and unwanted actions, including:

- "Phoning home" information about you, your computer and your surfing habits to a third party to use to spam you or push pop-up ads to your screen
- Open up your computer to a remote attacker using a RAT—a Remote Access Trojan—to remotely control your computer
- Capture every keystroke you type—private or confidential emails, passwords, bank account information—and report it back to a thief or blackmailer
- Allow your computer to be hijacked and used to attack a third party's computers in a denial-of-service attack that can cost companies millions and make you liable for damages
- Probe your system for vulnerabilities that can enable a hacker to steal files or otherwise exploit your system.

The newest threat is that of large numbers of captured personal computers mobilized into "Bot Armies" and used to launch highly organized Distributed Denial of Service (DDoS) attacks aimed at disrupting major business or government activity. Individual PC users are never aware that their machine is being used to disrupt internet traffic. There is currently little or no recourse to a legal solution even if the occurrence can be monitored.

Many PC users have unwittingly loaded, or unknowingly had spyware downloaded onto their computers. This happens when a user clicks "yes" in response to a lengthy and often extremely technical or legalistic end user licensing agreement. Or it happens when a user simply surfs the web, where self-activating code is simply dropped onto their machines in what is known as a "drive-by-download."

*Spyware Harms Computer Performance*

The misuse of technology and hijacking of spyware is a real and present danger to security and privacy. Unfortunately, the ill effects of spyware do not stop there. Spyware seriously degrades computer performance and productivity.

Testing earlier this month at the PestPatrol research laboratory revealed that the addition of just one adware pest slowed a computer's boot time—the amount of time it took to start up and function—by 3.5 times. Instead of just under 2 minutes to perform this operation, it took the infected PC close to 7 minutes. Multiply that by

a large number of PCs and you have a huge productivity sink hole. Add another pest and the slow-down doubles again.

We also tested web page access, and again it took much longer once a pest was added to a clean machine. Almost five times longer in fact for a web page to load on an infected PC. The pest also caused 3 web sites to be accessed, rather than the one requested, and caused the PC to transmit and receive much greater amounts of unknown data—889 bytes transmitted compared to 281 transmitted from the clean machine, and 3086 bytes received compared to 1419 bytes received by the clean machine. This translates into significant increases in bandwidth utilization. Managing bandwidth costs money.

*Increased costs due to unnecessary consumption of bandwidth on*

individual PCs, and the necessary labor cost in rebuilding systems to ensure they are no longer corrupt is virtually unquantifiable. It's likely quite large. System degradation is time consuming for the individual PC user and even more so for network administrators managing corporate networks. Even new PCs straight from the factory come loaded with thousands of pieces of spyware, all busy "phoning-home" information about the user and slowing down computing speeds.

Users do not invite this spyware onto their machines and should not have to live with it. Clearly this level of infestation is stepping beyond the bounds of what is fair and reasonable.

*Solutions*

On the basis of our extensive work in this area, we at PestPatrol believe only a combination of consumer education and protection, disclosure through legislation, and active prosecution will provide the answer needed to address the spyware threat. None of these solutions by themselves is enough. While we advocate and applaud industry self-regulation, we do not believe that it alone will be speedy or dramatic enough to address the spyware problem.

The first line of defense is education and protection. Any individual or business connected to the Internet today has to realize they are part of a complex network that is inextricably intertwined. Creators of spyware take advantage of that fact, plus the knowledge that most PC users are not sophisticated technologists. As an industry, we have begun to make computer users aware of the spyware threat by the creation of and active outreach by several groups and organizations. PestPatrol is a founding member of the Consortium of Anti-Spyware Technology, or COAST, a non-profit organization of anti-spyware companies and software developers committed to best practices.

Consumer education about spyware and promotion of comprehensive anti-spyware software aimed at detecting and removing unwanted pests is fundamental to our outreach. Our efforts are modeled after the decade-long effort by anti-virus software companies to raise awareness about virus threats. However, we also acknowledge that consumers, precisely because of the insidious nature of spyware, can only do so much to protect themselves, and cannot be alone responsible for controlling the spread of spyware.

Which brings us to the second line of defense—disclosure legislation. All applications, including those that are bundled and downloaded along with free software and with legitimate commercial applications, should be readily identifiable by users prior to installation and made easy to remove or uninstall. It is this transparent disclosure, and the ability of consumers to decide what does and does not reside on their systems, that needs to be legislated. Consumers should have the ability to make fully informed decisions about what they choose to download onto their machines, while understanding the implications of doing so.

The third line of defense is aggressive prosecution. The deceptive practices employed by many spyware developers are already illegal under existing laws against consumer fraud and identity theft. Law enforcement agencies at the federal and state level should be encouraged to more aggressively pursue and prosecute those who clandestinely use spyware to disrupt service, steal data or engage in other illegal activity. A greater focus on spyware and the necessary allocation of resources to pursue this criminal activity is vital.

Spyware is a significant threat to the effective functioning and continued growth of the Internet. It is more than a nuisance. Given the dangers it represents, it is important that consumers, business and government work together to address the issue and safeguard the productivity and utility of the Internet computing environment.

I sincerely appreciate the opportunity to present my company's ideas on how to achieve this goal. Thank you.

PREPARED STATEMENT OF WEBROOT SOFTWARE, INC.

Webroot Software, Inc. appreciates the opportunity to provide written comments in conjunction with the Subcommittee's hearing on spyware. The hearing title is most appropriate. Spyware presents a serious problem for both the public and businesses, yet there is still minimum awareness about the significant risks associated with the rapid growth of spyware.

**Experts at Fighting Spyware**

Webroot Software, Inc., was founded in 1997 to provide computer users with privacy, protection and peace of mind. Today, Webroot provides solutions and services for millions of users around the world, ranging from enterprises, Internet service providers, government agencies and higher education institutions, to small businesses and individuals.

Among its award winning products is Spy Sweeper, winner of PC Magazine's 2004 Editors' Choice award. The magazine's objective review of 14 spyware detection products found: "Spy Sweeper is the most effective standalone tool for detecting, removing and blocking spyware." In the April 5 issue of Business Week, Stephen Wildstrom, author of the "Technology and You" column also recommended Spy Sweeper, referring to Webroot as the "established leader" in the market.

Webroot's world headquarters is located in Boulder, Colorado, with a European headquarters in Frankfurt, Germany, and sales offices in Chicago, London, Amsterdam, and Paris. Webroot products are sold online at www.webroot.com, and at leading retailers around the world, including Best Buy, CompUSA, Circuit City, Fry's, Staples and MicroCenter. In addition, Webroot provides a full suite of privacy and security solutions designed to help ISPs like Earthlink provide value-added products and services to their customers.

Every day, Webroot employees talk to computer users in the U.S. and Europe who are being negatively impacted by spyware that has found its way onto their computers. Webroot is on the front lines fighting spyware, but Congress and the Federal Trade Commission (FTC) have critical roles to play on this issue to increase public awareness, develop and reinforce clear rules, and actively enforce the law.

**Defining Spyware**

In 2003, Webroot helped to found the Consortium of Anti-Spyware Technology vendors (COAST), a non-profit organization established to facilitate collaboration among spyware detectors and increase awareness of the growing spyware problem.

COAST defines spyware as: **Any software program that aids in gathering information about a person or organization without their knowledge, and can relay this information back to an unauthorized third party.**

"Without your knowledge" and "to an unauthorized third party" are key components of this definition. The FTC recently held a workshop on spyware, which they appropriately titled: "Computer Monitoring Software on Your PC: Spyware, Adware, and Other Software." As the problem of spyware has grown, a slew of new words have surfaced. For informational purposes, we have attached as an appendix the glossary of spyware-related terms developed by COAST.

From a pure technology point of view, there is little difference between computer monitoring programs that serve legitimate purposes and those that put your privacy and personal information at serious risk. For example, a keylogger program like ChildSafe, a Webroot product, provides parents with the ability to monitor their childrens' online activities by tracking what the child types on the keyboard. A functionally similar keylogger program installed without permission by JuJu Jioang on computers in at least 15 Kinkos stores provided him with personal information about over 400 people, which he used to open back accounts and commit other illegal activities. Fortunately, that was one case that the government successfully investigated and prosecuted, but there are many more cases where the perpetrators are not yet identified, or even worse, where the victims do not even know they are victims.

Thus, there is not a technological definition for spyware. The definition is contextual—how the program came to reside on your computer is a threshold question to defining it as spyware.

**The Anatomy of Spyware**

There are many kinds of programs that fit within this definition of spyware. The COAST glossary attached as an appendix provides a more complete list, but there are four most common forms of spyware.

**Back Door Trojans** are malicious programs that appear as harmless or desirable programs. Back Door Trojans deploy remote access tools, allowing hackers to gain

unrestricted access to a user's computer. Trojans can be deployed as email attachments, or bundled with another software program.

**Keyloggers** are programs that can monitor and record the user's every keystroke. Key loggers can be used to gather sensitive data such as username and password, private communications, credit card numbers, etc.

**System Monitors** are applications designed to monitor computer activity. These programs can capture everything that is done on a computer. Information can be received at the computer, through remote access, or scheduled emails.

**Adware** is advertising supported software that displays pop-up advertisements whenever the program is running. Once installed, these programs will download and install new software and data files—advertisements, etc.—based on user activities such as websites visits.

Unlike a virus that many users get in the same way at the same time, spyware finds its way onto your computer through multiple channels at multiple times. Spyware may arrive bundled with freeware or shareware, through peer-to-peer downloads, attached to or embedded in email or instant messenger communications, as an ActiveX installation, or it may be placed on your computer accidentally or deliberately by someone with access to it. Once on your system, spyware secretly installs itself and goes to work.

Anti-virus software does not offer protection from spyware because spyware is not viral. Since it attaches itself to legitimate downloads, spyware can often pass easily through firewalls unchallenged. And by intertwining itself with files essential to system operation, spyware cannot be safely removed by simply deleting files with a system-cleaning tool.

In its most benign form, spyware can significantly slow systems down and result in more pop-up ads than usual. The more malicious spyware programs can lead to identity theft, theft of intellectual and other property, and data corruption. Unlike personalization or session cookies, spyware is difficult to detect, and difficult (if not impossible) for the average user to remove manually.

Some of the types of information collected by spyware programs without the knowledge of the computer owner are:

- Usernames and Passwords
- Electronic Assets
- Browsing Habits
- Applications Used
- Personal Information
- Email & IM Conversations
- IP and Trade Secrets
- Financial Records
- Customer Databases

Spyware can execute unwanted, unauthorized, and/or inappropriate code and use vital system resources. Spyware programs can be used to facilitate the unauthorized use of your machine for things like:

- Email Forwarding to Send Spam
- Background Computing
- Hacker Attacks

While some argue that spyware is installed with the user's knowledge (although the user may not understand exactly what s/he has done), most of the time it is installed surreptitiously as part of another program installation. Even if the bundling of software and information tracking practices are disclosed to the consumer through the End User License Agreement (EULA), such disclosures are rarely clear and conspicuous. Even when they exist, notices often fail to provide users with a real understanding of what information will be collected and how the entity collecting the information will use it.

**A Real and Growing Problem**

Earthlink and Webroot collaborated in the first quarter of 2004 to offer a free SpyAudit to Earthlink subscribers. On April 15, 2004 the companies jointly released the findings for January 1, 2004 through March 31, 2004. During that timeframe, 1,062,756 spyware scans were run, identifying a total of 29,540,618 instances of spyware, meaning roughly 28 instances of spyware per PC. Of particular concern, were the large number of System Monitors and Trojans found which accounted for 369,478 of all the spyware instances found.

Expert reports have estimated that 9 out of 10 PCs in the United States are infected with spyware. Studies have often showed that spyware is growing at a much faster rate than computer viruses.

**Responding to Spyware**

The unfortunate reality is that there is probably no way to completely eradicate spyware. The Internet is global, which makes establishing and enforcing legal standards challenging. There are also significant economic drivers that make the creation and dissemination of spyware very appealing to many people, both in the U.S. and abroad. The combination of a profit-driven motivation, coupled with the vulnerability of personal information, makes spyware unique and more threatening than many other online security and privacy concerns, like viruses and spam, which the government has addressed in the past several years.

It is clearly going to take a combination of technology, public education, sound public policy and strong enforcement to address this problem. To that end, we applaud the efforts of Congresswoman Bono, Congressman Towns, Senators Burns, Boxer and Wyden and the FTC to call attention to the serious negative impacts that spyware can have on the public and the economy. Increased awareness and education about spyware is essential to effectively deal with the problem.

Certainly, regulating technology-related issues is inherently tricky, but this is not an issue that will go away by itself, and industry self-regulation is unlikely to adequately address the issue in a reasonable time frame. Congress has an opportunity to address this issue before it becomes debilitating. H.R. 2929 and S. 2145 offer alternative approaches, both with good qualities. We urge that this issue not be set aside to resolve itself—because it won't. We are on the front lines of this arms race, and we need reinforcement in the form of clear rules related to spyware to help us effectively fight for businesses and consumers who need to retain control over their PCs.

We appreciate the opportunity to share our views with the Subcommittee.

GLOSSARY OF SPYWARE RELATED TERMS DEVELOPED BY THE CONSORTIUM OF ANTI-SPYWARE TECHNOLOGY VENDORS

**Adware:** Often used as a term for spyware, it is preferred and used by makers of software that include ad-serving mechanisms. Adware is advertising-supported software that displays pop-up advertisements whenever the program is running.

**Browser Helper Object (BHO):** A small program that runs automatically every time an Internet browser is launched. Generally, a BHO is placed on the system by another software program and is typically installed by toolbar accessories. They can track usage data and collect any information displayed on the Internet.

**Bundled:** An arrangement in which one or more software programs are included with another program, for technical reasons or because of a business partnership. Many instances of spyware installations come through bundling.

**Cookie:** A mechanism for storing a user's information—such as login information and passwords, or a user's previous activity on a site—on a local drive.

**Dialers:** Dialers are software that, once downloaded, disconnects the user from his or her modem's usual Internet service provider, connect to another phone number, and the user is then billed.

**Drive-by Download:** While not a piece of spyware itself, this misleading dialogue box serves as a gateway for the stealth installation of spyware applications. In some cases, spyware can be installed even if the user does not choose the "yes" or "accept" button.

**File-sharing programs:** These are software applications that allow the exchange of files (especially music, games, and video) over a public or private network. See Peer-to-Peer.

**Freeware:** Software that can be downloaded and shared at no cost.

**Hijacker:** Hijackers typically come in two categories, **Browser/Page Hijackers** and **System Hijackers:**

**Browser/Page Hijackers:** Applications that attempt to take control over a user's home page or desktop icons, resetting them to a pre-determined website destination.

**System Hijacker:** Software that uses the host computer's resources to proliferate itself or use the system as a resource for other activities. This taxes the host computer's resources, negatively affecting computer and Internet speeds.

**KeyLoggers**—See **System Monitors.**

**Opt-in:** An online process by which a user chooses to receive information (such as e-mail newsletters) or software, often by checking a check box on a Web page or software installation screen.

**Opt-out:** An online process (such as un-checking a pre-checked box) by which a user actively chooses not to receive information, such as e-mail newsletters or software. Actively opting out will prevent a user's information from being a shared with businesses.

Users should be warned that most "opt-out" options are actually a scam that serves to confirm legitimate/active email addresses. Privacy experts recommend that users do not use the "opt-out" option unless they are personally familiar with the company where the email originated.

**Parasite:** A parasite is unsolicited commercial software or programs installed on a computer for profit without the consent or knowledge of the user.

**Parasiteware:** Parasiteware is the term for any Adware that by default overwrites affiliate-tracking links. This behavior is viewed as parasitic because this software diverts affiliate commissions and credits the affiliate's income to another party. To the end user, Parasiteware is not a serious security threat. See Thiefware.

**Peer-to-peer (P2P):** A method of file sharing over a network in which individual computers are linked via the Internet or a private network to share programs/files, often illegally. Users download files directly from other users' computers, rather than from a central server.

Many P2P programs bundle third-party advertising programs, and are currently the second largest source of virus, Trojan and data mining infections.

**Remote Administration Tools/ RATs:** Some Trojans, called RATs (Remote Administration Tools), allow an attacker to gain unrestricted access of a computer whenever the user is online. The attacker can perform activities such as file transfers, adding/deleting files, and controlling the mouse and keyboard.

**Scumware:** A slang term for spyware or any unwanted software/programs installed on your computer.

**Shareware:** Software that is distributed—usually via the Internet and or CD-Rom—for free and on a trial basis.

**System Monitors/Keyloggers:** These applications are designed to monitor computer activity to various degrees. They can capture virtually everything a user does on his or her computer, including recording all keystrokes, emails, chat room conversations, web sites visited, and programs run.

**Thiefware:** Thiefware applications steal affiliate commissions by either overwriting tracking cookies or spawning new windows to redirect traffic from search engine keywords or other websites. This practice, while not currently illegal, is considered unethical among those in the merchant/affiliate community. See Parasiteware.

**Tracking Cookies:** Not to be confused with personalization cookies (which allow users to customize pages and remember passwords), some web sites now issue tracking cookies. Tracking cookies allow multiple web sites to store and access records that may contain personal information (including surfing habits, user names and passwords, areas of interest, etc.), and subsequently share this information with other web sites and marketing firms.

**Trojan Horses:** Trojans are malicious programs that appear as harmless or desirable applications. Trojans are designed to be actively harmful to PCs by intentionally damaging PC operating systems, other software or hard drives. Trojans are generally distributed as email attachments or bundled with another software program (often fraudulent versions of legitimate software).

**Web bugs:** A file, usually a small or invisible graphic image, that is placed on a Web page or in e-mail to allow a third party to monitor user behavior.

---

## DOWNLOADING SHARED FILES THREATENS SECURITY

by Sgt. 1st Class Eric Hortin

FORT HUACHUCA, Ariz. (Army News Service, April 22, 2004)—People spend hours in front of their computer screen, downloading music or new movies from the Internet, and not paying a cent, the Army considers such action on government computers to be a security threat.

One program that is used to downloaded files is Peer-to-Peer (P2P) architecture. It is a type of network in which each workstation has the capability to function as both a client and a server. It allows any computer running specific applications to share files and access devices with any other computer running on the same network without the need for a separate server. Most P2P applications allow the user to configure the sharing of specific directories, drives or devices.

In a white paper written by the Army's Computer Network Operations Intelligence section, unauthorized P2P applications on government systems, "represent a threat to network security."

"The idea of someone else getting unfettered access to anything of yours without your explicit consent should scare anybody—and that's exactly what P2P authorizes," says Zina Justiniano, an intelligence analyst with the U.S. Army Network En-

terprise Technology Command's (NETCOM) Intelligence Division, G2. "P2P is freeware. Freeware, shareware—most of the stuff that you pay nothing for, has a high price. The fact that it's free says that anybody and their cousin can get it; that means that anybody and their cousin can get to your machine." P2P applications are configured to use specific ports to communicate within the file sharing "network," sometimes sidestepping firewalls. This circumvention creates a compromise and potential vulnerabilities in the network that, in a worse case scenario, can lead to network intrusions, data compromise, or the introduction of illegal material and pornography. There is also the issue of bandwidth. Since the start of the global war on terrorism, the most pressing issue from service members in the field has been the shortage of bandwidth to transmit battlefield intelligence to combatant commanders. The average four-minute song converted into an audio file recorded at 128-bit, can be upwards of 5 megabytes. Full-length video MPEG files can easily reach 1.6 gigabytes. Depending on the connection speed, even a small file may take several minutes to hours to download, using valuable bandwidth. Unauthorized use of P2P applications account for significant bandwidth consumption. It limits the bandwidth required for official business, and storage capacity on government systems. While those who monitor the Army networks agree that copyright infringement is a valid issue, they do have other, more important concerns.

There are several known Trojan horses, worms and viruses that use commercial P2P networks to spread and create more opportunities for hackers to attack systems. Trojan horse applications record information and transmit it to an outside source. They can also install "backdoors" on operating systems, transmit credit card numbers and passwords—making these malicious programs a favorite of hackers. Some of the malicious codes allow hackers to snoop for passwords, disables antivirus and firewall software, and links the infected system to P2P networks to send large amounts of information (spam) using vulnerabilities in Windows operating systems.

"If it's a really good Trojan horse, it will actually run two programs; it will run the program they said they were going to run, so they will not only download it, but they will install it and be very happy that it's there," Justiniano said. "Meanwhile in the background, another program is doing malicious damage to the computer by either damaging files or possibly taking files off the computer without your knowledge. If it's a really nice program that runs well, (the user) will pass that file over to someone else because they really got their money's worth out of it. People will just keep passing it along."

Trojan horses are not the cause of all security issues. Oftentimes, "spyware" applications are installed with the users consent; it's buried in the really long agreement that nobody reads that a user must click, "I Accept," in order to begin the installation. This is especially true with free-ware applications downloaded from the Internet. According to published reports, a couple of years ago, some P2P applications came packaged with a spyware application that acted as a Trojan horse. This specific program sent information to an online lottery server.

Those are just a couple of reasons the Army doesn't want its people loading P2P on their systems, and enacted regulations prohibiting loading those applications.

The Army's regulation on Information Assurance, Army Regulation 25-2, specifically prohibits certain activities; sharing files by means of P2P applications being one of them. There are some, however, who have P2P applications on their Army systems and use them despite the prohibition of such activities.

Over a two-month period at the end of last year, government organizations identified more than 420 suspected P2P sessions on Army systems in more than 30 locations around the globe.

It seems some don't understand or haven't read the standard Department of Defense warning that says, "Use of this DOD computer system, authorized or unauthorized, constitutes consent to monitoring." For those who think, "How are they going to know it's me? I'm just one person in a network of hundreds of thousands," don't be surprised when network access is cut off and the brigade commander is calling.

It is the role of the Theater Network Operations and Security Center, located in Fort Huachuca, Ariz., to monitor and defend its portion of the Army network. This includes identifying potential security risks to the network, and unauthorized P2P applications, which create a considerable risk to those networks.

"People shouldn't assume they are using P2P applications in secrecy," said Ronald Stewart, deputy director of the C-TNOSC. "We are able to detect use of P2P, and when we do, we take measures. We can detect and identify systems with P2P software on them; and when we find them, we direct the removal of the software from the system through the command chain."

Some Soldiers try to work around the Army networks to feed their P2P habits. Lt. Col. Roberto Andujar, director of the C-TNOSC, says using the Terminal Server

Access Controller System (TSACS) to dial into the military network is not a workaround, because there are tools in place to identify P2P traffic.

Methods commonly used by commercial industry, such as Internet Protocol (IP) address and port blocking, random monitoring, and configuring routers are some of the methods the C-TNOSC and installations take to prevent P2P access. There are other methods used, but specific examples cannot be discussed.

Commanders who unwittingly allow P2P to run unchecked on their networks are not exempt from liability. Commanders may be held personally liable for any illegal possession, storage, copying, or distribution of copyrighted materials that occurs on their networks. Soldiers, civilian employees and contractors face even tougher penalties.

People using P2P on government computers can to look forward to other possibly harsher punishments depending on the kinds of files the users are sharing.

"Say you have a Soldier downloading music through P2P, in violation of copyright rules," said Tom King, a legal adviser with NETCOM. "The people who own the copyright can actually sue that Soldier. Then you have the issue that he's violating a lawful order. Then you have the issue that it's a misuse of government time and misuse of a government resource. He can be in a world of hurt. Then he's also exposing the Army network to hacking attacks."

"Prosecutions are on the rise. Discipline is on the rise. People are taking this stuff more and more seriously all the time," King said. "People just don't understand that there's a price to be paid for this."

Not understanding seems to be the main reason P2P applications keep showing up on Army computer systems.

"User education is one of the keys," said Kathy Buonocore, chief of the Regional Computer Emergency Response Team. "Some users don't know it's illegal."

"When I call some commanders and tell them, they say, 'What's P2P?'" Andujar said. "Commanders have to be educated and take action."

Education has to extend down to the organization administrators. Justiniano says those who have administrator privileges on government computer systems are the ones loading the unauthorized programs. To prevent this, system and network administrators should configure systems correctly, so users cannot install unauthorized software.

"There are very few benefits that are not addressed somewhere else, that do not include the risk of P2P software," Justiniano said, adding that the use of Army Knowledge Online knowledge centers and secure File Transfer Protocol sites are their preferred method of file sharing.

(Editor's note: Sgt. 1st Class Eric Hortin is a journalist for the U.S. Army Network Enterprise Technology Command.)

○