AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

COMBATING SPYWARE: H.R. 29, THE SPY ACT

HEARING

BEFORE THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

JANUARY 26, 2005

Serial No. 109–10

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

99–899PDF WASHINGTON : 2005

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*

RALPH M. HALL, Texas
MICHAEL BILIRAKIS, Florida
Vice Chairman
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
NATHAN DEAL, Georgia
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
ROY BLUNT, Missouri
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
C.L. "BUTCH" OTTER, Idaho
SUE MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee

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
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MIKE DOYLE, Pennsylvania
TOM ALLEN, Maine
JIM DAVIS, Florida
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Texas
MIKE ROSS, Arkansas

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

(II)

CONTENTS

	Page
Testimony of:	
Baker, David N., Vice President, Law and Public Policy, Earthlink, Inc	14
Rubinstein, Ira, Associate General Counsel, Microsoft Corporation	17
Schmidt, Howard A., President and Chief Executive Officer, R&H Security Consulting	24
Schwartz, Ari, Associate Director, Center for Democracy and Technology	28
Material submitted for the record by:	
Information Technology Association of America, white paper entitled, Spyware, Supportware, Noticeware, Adware and the Internet	57
Webroot Software, Inc., prepared statement of	54

COMBATING SPYWARE: H.R. 29, THE SPY ACT

WEDNESDAY, JANUARY 26, 2005

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
WASHINGTON, DC.

The committee met, pursuant to notice, at 10:23 a.m., in room 2123 of the Rayburn House Office Building, Hon. Joe Barton (chairman) presiding.

Members present: Representatives Barton, Hall, Stearns, Gillmor, Deal, Whitfield, Cubin, Shimkus, Shadegg, Pickering, Buyer, Radanovich, Pitts, Walden, Terry, Ferguson, Rogers, Otter, Myrick, Murphy, Burgess, Blackburn, Markey, Towns, Eshoo, Stupak, Wynn, Green, Strickland, Schakowsky, Solis, Gonzalez, Inslee, Baldwin, and Ross.

Staff present: Bud Albright, staff director; Andy Black, deputy staff director; David Cavicke, chief counsel; Chris Leahy, policy coordinator; Shannon Jacquot, counsel; Will Carty, professional staff; Billy Harvard, legislative clerk; Julie Fields, special assistant to policy coordinator; Consuela Washington, minority senior counsel; and Ashley Groesbeck, research assistant.

Chairman BARTON. The committee will come to order.

Good morning, and welcome to all members and guests for the first hearing of the Energy and Commerce Committee for the 109th Congress.

I want to welcome our new members on both sides of the aisle. We will have a formal recognition of each of you at the appropriate time when the former Chairman Dingell is here. He is in a Democratic Leadership meeting and may not be able to attend. So we will save the formal introductions for another time.

Today, our committee is going to receive testimony on legislation to protect consumers against Internet spying. Legislation, I should add, that last year passed through this committee on a 45-5 vote, and then on the House floor 399-1. Not only did the bill receive overwhelming support from our members, but from many technology companies and associations, including Yahoo, eBay, AOL TimeWarner, Dell, Microsoft, EarthLink, and the U.S. Telecom Association.

The reason for the broad support of the bill is evident: the problem of Internet spying has grown to a critical point. Internet and technology companies are swamped by complaints and calls from their customers, not only asking for help in cleaning their computers of these programs, but also expressing real anger that their machines are continually slowed or stopped by simply navigating the Internet.

I have a personal experience of this. My daughter, Kristen, who just graduated from college, bought a brand-new computer last year, and it is totally worthless today because of spyware that has infected her computer. She recently decided to junk that computer and buy a new computer.

Many consumers remain unaware of how these applications end up on their computers and remain unable to remove them because of deceptive or nonexistent instructions for un-installing them.

Losing some level of control of your own personal property is bad enough, but when added to the likelihood that these programs are monitoring your computer usage and transferring, possibly, your own private information to third parties without your permission, the spyware problem rises to a dangerous level. Many of these violations constitute a trespass-like offense, and in the worst cases, facilitate theft and fraud. Information gathered by spyware programs can be used to further slow your computer by bombarding you with pop-up ads and the collection of personal information can be used to steal your money, your identity, or both.

All members, their families, and their constituents have become susceptible to this problem. Even many of our committee computers here on the Hill have been hampered by spyware's ill effects. This is a problem that must be addressed quickly, and given the interstate nature of e-commerce, it must be addressed by Federal legislation. I am encouraged that the Federal Trade Commission is finally beginning to take action against some of the worst actors in the spyware area, but Congress must also act quickly to give the FTC the additional power it needs to stem the tide of Internet monitoring. Last year, as I mentioned, we succeeded in passing this bill through the House, but the Senate failed to act. I am hopeful that that will not be the case this year, and I have been in contact with several Democrat and Republican Senators, and they say that they are going to move the bill very quickly.

I want to commend a number of members for their outstanding leadership on this issue. Our No. 1 leader, Congresswoman Mary Bono of California, is not here today, because she is ill in California with a severe case of bronchitis, so she couldn't make it back to Washington for the hearing today. But I do want to commend her for her leadership. She introduced this legislation in 2003, when most of us had never heard of spyware, and has worked tirelessly to ensure its passage. I also want to commend Congressman Ed Towns, he is here today, for his leadership. He co-sponsored with Congresswoman Bono this legislation in our committee, and he, too, has worked tirelessly in a bipartisan manner to make this an excellent piece of legislation. I also want to thank our subcommittee chairman Congressman Stearns and also our ranking member, the gentlelady from Illinois, Mrs. Schakowsky. She has done an excellent job in drafting this bill.

These members, as well as Congressman Dingell, have worked diligently to bring this legislation to the floor last year, and I hope we can move just as quickly and just as cooperatively this year to put this legislation through the House and send it to the Senate and encourage the Senate to act.

I am also encouraged by the participation of a number of industry groups. We have drawn on their expertise in crafting this legis-

lation. I encourage them to continue to work with us to combat spyware on a technological and a consumer educational level. It will take a mix of technology, consumer awareness, industry best practices, and strong enforcement to effectively fight spyware. I want to thank those who have worked with us throughout the process and those that are participating in our hearing today.

I would now yield, since Mr. Dingell is not here, to Ms. Schakowsky, the subcommittee ranking member, for an opening statement, and then we will go to Mr. Stearns.

Ms. SCHAKOWSKY. Thank you, Mr. Chairman. I would like to first also welcome our new members and particularly thank the new Democratic members who made it possible for me to rise to this lofty position in the second row and close to the chairman. This is a big day for me. And I wanted you—to thank you, Chairman Barton, for holding this hearing on H.R. 29, the SPY ACT, a strong, pro-consumer, bipartisan piece of legislation, which addresses one of the newest and most troublesome consumer and privacy issue: spyware. And I would also like to thank Ranking Member Dingell, who is unable to be here today. And as the ranking Democrat on the Commerce Trade and Consumer Protection Subcommittee in the 108th Congress, I had the privilege of working closely with my Chairman, Chairman Stearns, along with Representative Towns and Bono on the first version of the SPY ACT.

As we learned last year, spyware, while not yet a household word, is a household phenomenon. The recent—a recent study by America Online found that 80 percent of families with broadband access had spyware on their computers. EarthLink, one of our witnesses here today, along with Web Route, an anti-spyware software provider, found that in 3 million scans of computers, there was an average of 26 instances of spyware on each and every computer. With those kinds of numbers, spyware will soon be a part of everyone's vocabulary.

However, because of the surreptitious nature of spyware, because of the furtive practices of the spyware purveyors, many people have no idea that their computers have been infected with the software. People notice that pop-up ads will not go away and they notice when their computers are much slower. And of course, they notice when their home pages have been changed, but not by them. Consumers tend to blame viruses, their—on their old computer or their Internet service providers. But because spyware is bundled with software people do want to download, and because it is drive-by downloaded from unknowingly visiting the wrong website, people do not know that, in many cases, the real cause of their headaches is spyware.

As we pointed out last year, spyware is much more than merely annoying. Slow computers and pop-up ads are just symptoms of the real trouble spyware can cause. The software is so "resourceful" that it can snatch personal information from computer hard drives, track every website visited, and log every keystroke entered. Spyware is a serious threat to consumer privacy and potentially a powerful tool for identity theft, a serious crime that is on the rise. Although we do not want to stop legitimate uses of the software underlying spyware, like allowing easy access to online newspapers, we do want consumers to have control of their computers

and personal information and to stop truly nefarious uses of the programs.

The SPY ACT finds the balance that helps protect consumers from truly bad acts and actors while preserving the pro-consumer functions of the software. It prohibits indefensible uses of the software, like keystroke logging, and it gives consumers the choice to opt in to the installation or activation of information-collection software on their computers, but only when consumers know exactly what information will be collected and how it will be used.

Furthermore, the SPY ACT gives the FTC the power it needs, on top of laws already in place, to pursue predatory uses of the software. The SPY ACT puts the control of computers and privacy back in consumers' hands, and I am glad that we are moving the bill forward once again.

And once again, I thank my colleagues for this pro-consumer, pro-privacy, and bipartisan piece of legislation, and I look forward to working with you again this year.

Thank you, Mr. Chairman.

Chairman BARTON. Thank you.

We would now like to recognize the subcommittee chairman, Mr. Stearns, for an opening statement.

Mr. STEARNS. Good morning. And thank you, Mr. Chairman.

I am pleased that H.R. 29 is the first order of business. I commend you for bringing it forward. I also hope that the Senate will pass this anti-spyware legislation so that we can arm the Federal Trade Commission with a strong Federal response to combat this growing problem before it gets out of control. The elimination of spyware and the preservation of privacy for the consumer are critical goals if the Internet is to remain safe, reliable, and a credible means of commerce for the United States and the rest of the world.

We know "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. And while I would like to believe that something this egregious should fall easily into the "I know it when I see it" category, spyware is a little bit different, my colleagues. It allows unwanted software programs or spies to break, undetected, into our private lives to snoop, steal, and manipulate our online activities right under our noses.

The spy and this software also makes identifying and finding those unwelcome guests a challenge. In fact, the burden of disinfecting corrupt computers usually falls on the consumer, who, in turn, usually contacts the closest available support center, often thinking they have had—they have a hardware or software problem. The typical scenario takes an obvious toll on our productivity and the engine of commerce.

It is important to note that the bill before us today, H.R. 29, is identical to the one that we passed in Congress by a 45-5 vote in the full committee, and in the House, 399-1. This bill has been crafted to target obvious spyware abuses, like keystroke logging. The bill also goes after offenders hidden in the shadow of confusing licensing agreements and other less obvious means of deception and trickery intended to defraud the computer. Specifically, the bill does the following: prohibit deceptive practices, like keystroke logging, web page hijacking, and unsolicited ads that can't be deleted;

establishes a clear opt-in for consumers wishes to download monitoring software, and requires that such software be easily disabled; three, creates penalties with heavy monetary penalties that should make fraudsters think twice before they act; and finally, reestablishes a uniform, national rule regulating spyware because of the inherently interstate nature of interstate commerce—Internet commerce.

Another challenge we face is ensuring that a response to the growing spyware problem does not penalize legitimate uses of similar information technology designed to monitor and prevent unauthorized activity. For example, programs designed to help parents monitor the online activity of their children and legitimate online marketing techniques all use similar technologies in an inoffensive and legal manner. This committee understands that there are gray areas, Mr. Chairman, with spyware, and as a result has worked very hard and it is a credit to the subcommittee staff and what they have done here to try to negotiate to focus this bill on the bad actors while preserving the legitimate use of these technologies.

But there are some concerns to H.R. 29: examining the need for an exception for cookies and the issue raises—raised by third-party cookies, since the bill is intended to apply only to software; two, looking at ways to compute damages that are realistic and not excessive so that we don't obstruct and stop the Internet explosion; and finally assessing whether the definition of "information collection program" adequately captures advances in the technology. These are obtuse, very difficult to understand a third-party cookie and how it works in the computer, but again, we do not want to necessarily stop these third-party cookies from working.

This is a balanced bill, though, and I think we need to move forward. I think it will achieve our goals. I would like to thank the distinguished witnesses this morning for attending and assisting us in discussing and debating this. And I also want to recognize Chairman Barton for his vision and his leadership, and of course, as he has mentioned, Ms. Bono of California and Mr. Towns. I would also like to thank my subcommittee ranking member, Ms. Schakowsky and Mr. Dingell for his support.

And with that, Mr. Chairman, I conclude.

[The prepared statement of Hon. Clifford Stearns follows:]

PREPARED STATEMENT OF HON. CLIFFORD STEARNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Thank you Mr. Chairman.

Good morning. I am very pleased that H.R. 29, the "Securely Protect Yourself Against Cyber Trespass Act" or "Spy Act" is the first order of business for this great Committee as we start the 109th Congress. Enacting meaningful anti-spyware legislation is a priority, and therefore, it is fitting that the Committee get focused early on the important work necessary to pass this bipartisan bill during this Congress. I also would like to call on our Senate colleagues to pass similar anti-spyware legislation soon so that we can arm the Federal Trade Commission with a strong federal response to combat this growing problem before it gets out of control. The elimination of spyware and the preservation of privacy for the consumer are critical goals if the Internet is to remain a safe, reliable, and credible means of commerce for the United States and the rest of the world.

As we now know, 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. And while I'd like to believe that something this brazen and egregious should easily fall into the "I know it when I see it category," spyware is different—it allows unwanted software programs or "spies" to break undetected

into our private lives to snoop, steal, and manipulate our online activities right under our noses. The "spy" in this software also makes identifying and finding these unwelcome guests a challenge. In fact, the burden of disinfecting corrupted computers usually falls on the consumer, who in turn usually contacts the closest available support center often thinking they have a hardware or software problem. This typical scenario takes an obvious toll on our productivity and the engine of commerce.

It is important to note that the bill before us today, H.R. 29, is identical to the one that passed in the last Congress by a 45-5 vote in this Committee and by 399-1 in the full House. And while H.R. 29 has been crafted to target obvious spyware abuses, like keystroke logging, the bill also goes after offenders hidden in the shadows of confusing licensing agreements and other less obvious means of deception and trickery intended to defraud the consumer. Specifically, H.R. 29 does the following:

- Prohibits deceptive practices like keystroke logging, web page hijackings, and unsolicited ads that can't be deleted.
- Establishes a clear opt-in for consumers wishing to download monitoring software, and requires that such software be easily disabled.
- Creates penalties with teeth- heavy monetary penalties that should make fraudsters think twice before they act.
- And reestablishes a uniform national rule regulating spyware because of the inherently interstate nature of Internet commerce.

Another challenge that we face as legislators is ensuring that our responses to the growing spyware problem don't penalize legitimate uses of similar information technology designed to monitor and prevent unauthorized activity. For example, programs designed to help parents monitor the online activity of their children and legitimate online marketing techniques all use similar technology in an inoffensive and legal manner. This Committee understands that there is a gray area with spyware, and as a result, has worked very hard to focus this bill on the bad actors while preserving the legitimate use of these technologies. Among some of the concerns expressed regarding H.R. 29 that will be examined as we continue to work on the bill are:

- Examining the need for an exception for cookies and the issues raised by third party cookies since the bill is intended to apply only to software.
- Looking at ways to compute damages that are realistic and not excessive.
- Assessing whether the definition of "information collection program" adequately captures advances in the technology.

This is a good, balanced bill that is needed to protect the online consumer from those with malicious intentions and to blow the cover of the "spies" residing in our personal property - our PERSONAL computers. I believe that H.R. 29 will achieve just that, and I continue to support its passage.

I would like to thank the distinguished panel of witnesses before us today for assisting the Committee's important work to discuss, debate, and explore the issues at hand to achieve a balanced but aggressive solution.

In closing, I'd like to recognize Chairman Barton for his vision and leadership on this issue. I'd also like to commend, in particular, Ms. Bono of California, for bringing the issue of spyware to the fore, and for her dedication to protecting the consumer. I also would like to recognize my Democratic colleagues, especially Mr. Dingell, Ms. Schakowsky, and Mr. Towns and their staffs for their help in making H.R. 29 a truly bipartisan effort and a pleasure to work on.

Once again, I would like to welcome the witnesses today and look forward to their testimony. Thank you.

Chairman BARTON. I thank the gentleman.

I would now like to recognize Mr. Markey of the World Champion Boston Red Sox and, perhaps, the World Champion New England Patriots for an opening statement.

Mr. MARKEY. Mr. Chairman, we are the World Champion Boston Patriots, and we are going to continue being the World Champion Boston Patriots. So we are——

Chairman BARTON. I ask unanimous consent to revise.

Mr. MARKEY. We are—we can't believe it, either, so thank you, Mr. Chairman. And thank you for having this hearing today, and Mr. Dingell. Mr. Stearns and Ms. Schakowsky have done an excellent job in shepherding this bill through, and I want to congratu-

late Mr. Towns and Ms. Bono for their leadership on this very important issue.

The online villains who spread spyware deceive computer uses through disingenuous download requests, phony icons and covert tricks to induce users to permit the installation of programs that computer users do not want or require. In contrast to software applications from reputable online companies, surreptitiously installed spyware programs are designed to thwart a user's ability to control their own computers. Rather than improving a computer's online experience, the installed features often deliver annoying pop-up ads, hijack home pages, and can secretly monitor a consumer's use of their computer and their travels across the Internet. Hopefully we can move this consensus bill through the process and have the Senate side produce spyware legislation this session as well.

In addition, I would also like to note that I look forward to working with Chairman Barton and our other committee colleagues on privacy legislation this year. In the last session, I offered legislation to extend the Cable Act's privacy protections to other similar entities. I was successful in getting one portion of my bill enacted, namely extending these consumer privacy protections to satellite providers, such as DirectTV and EcoStar, as part of the Home Satellite Viewer Act legislation that became law last year. Yet, we need to pass the remaining part of my bill to close the current loophole, which leaves consumers of services such as Replay TV with no legal privacy protections. What consumers watch at home, how they use the Internet, who they call or e-mail, and what services they may subscribe to are nobody's business. And companies should not monitor, collect, and disclose such personal information without the prior knowledge and express approval of consumers.

So I intend to reintroduce my privacy bill regarding Replay TV and other such devices, and I hope that we can work on that and similar online privacy legislation this year. I thank you, again, Mr. Chairman, for having this very important hearing today.

Chairman BARTON. Thank you, Mr. Markey.

We would now like to recognize the gentleman from Ohio, Mr. Gillmor, for a 3-minute opening statement.

Mr. GILLMOR. Mr. Chairman, I will waive, other than to say that I am very happy to see the opt-in requirement in this legislation.

Chairman BARTON. Okay.

We would recognize the gentleman from New York, the original cosponsor of the bill in the last Congress, Mr. Towns.

Mr. TOWNS. Thank you very much, Mr. Chairman, for holding this hearing today.

I greatly appreciate the commitment you have shown to address this important issue and this legislation. As the primary Democratic sponsor, I have been proud to work with Congresswoman Mary Bono, the author of this bill, and I hope she recovers really, really soon from her illness. Her leadership, insight, and persistence on the spyware problem have been unmatched. I salute her for her continued hard work on this legislation.

When we first embarked on this legislative process, spyware was a growing consumer nuisance. Most people had no idea what it was. They had no idea that software could be downloaded on their

computer without their knowledge and record and transmit their personal information. Now the problem is so widespread, it is hard to find someone who has not been negatively affected by spyware. In fact, the day the spyware act was on the House floor last year, my daughter called me to say that a computer had just crashed due to spyware and indicated that something needs to be done to rectify this problem. And I informed her that we were working on it as we were talking.

Last year, with Chairman Barton and Ranking Member Dingell's leadership——

Chairman BARTON. You just lost your microphone.

Mr. TOWNS. Last year——

Chairman BARTON. Oh, I am sorry. I inadvertently hit the mute button.

Mr. TOWNS. So you are part of spyware.

Last year, with the chairman and the Ranking Member Dingell's leadership, the bill passed the House floor. This year, by getting a much earlier start, I believe Congress can put a bill on the President's desk to provide consumers with additional tools to protect the consumer from spyware.

This is not only critical for consumer privacy, but it is also essential to ensure the integrity of e-commerce. Throughout this process, we have made several modifications to the bill to target bad actors while preserving technological applications. I look forward to hearing from today's witnesses on this.

And of course, Mr. Chairman, on that note, I yield back.

Chairman BARTON. I thank the distinguished gentleman from New York and point out that is the first time in my tenure as Chairman that I have used the mute button, even if inadvertently, and I hope it is the last time.

Does the gentlelady from Wyoming seek to make an opening statement?

Ms. CUBIN. I will submit.

Chairman BARTON. Okay. Does the gentlelady from California, Ms. Eshoo, seek to make an opening statement?

Ms. ESHOO. Mr. Chairman, I am going to place my statement in the record. I want to thank everyone that was involved in this. As some members might recall, when the bill was being marked up last year, I had some serious concerns and expressed those to my colleagues on the committee, and I thank them for paying attention to what we have put forward. And I think that we have a strengthened effort, and this should be not only passed by our committee but by the full House, and I look forward to that. So thank you, and here is to the 109th Congress to this committee distinguishing itself, as it has in the past. And I wish you and all of the subcommittee chairmen and ranking members my best and will do everything I can to bring even more credit to this committee and welcome to the new members.

Chairman BARTON. Thank you.

Ms. ESHOO. Thank you.

[The prepared statement of Hon. Anna G. Eshoo follows:]

PREPARED STATEMENT OF HON. ANNA G. ESHOO, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. Chairman, I'm very pleased that the Committee is considering H.R. 29, the Spy Act, a bill which I'm proud to support.

The word "spyware" raises eyebrows and causes anxiety for almost anyone that uses computers and the Internet, particularly those of us that have had their computer's hijacked, or know someone that has. But as we've learned, there are many "monitoring" or "information gathering" activities that are really benign and actually enhance a user's experience on the Net or with their computer. In fact, some of these activities are essential to protect personal computers from hackers or viruses.

As my colleagues will recall, I was very concerned about the spyware legislation considered by the Committee during the last Congress (H.R. 2929), and I opposed this bill during Committee markup. I believed our consideration then was rushed, and that too many important issues were left unresolved, putting at risk many of the services and security features that consumers value and rely on.

Subsequent to the Committee's consideration, Representative Issa and I se nt a letter to the Chairman and Ranking Member identifying our most significant concerns. I'm pleased that the Chairman, Mr. Dingell, and the bill's sponsors were very responsive to these concerns and that we were successful in putting an improved bill before the House last session. Unfortunately, the Senate never acted on this legislation.

Once again, I'd like to thank the Chairman, the Ranking Member, Rep. Bono, Rep. Towns, and their staffs for their hard work on this legislation and their willingness to work with me to improve this bill and eliminate any unintended consequences.

I look forward to hearing from the witnesses and working with my colleagues to pass H.R. 29 through Committee, and bring it back to the House floor.

Chairman BARTON. Thank you.

Does the gentleman from Pennsylvania, Mr. Pitts, wish to make an opening statement?

Mr. PITTS. No, thank you.

Chairman BARTON. Does the gentleman from Michigan, Mr. Stupak, wish to make an opening statement?

Mr. STUPAK. No, thank you.

Chairman BARTON. Does the gentleman from Oregon wish to make an opening statement?

Mr. WALDEN. No, thank you, Mr. Chairman. I will reserve.

Chairman BARTON. Does the gentleman from Maryland, Mr. Wynn, wish to make an opening statement?

Mr. WYNN. No.

Chairman BARTON. Okay. Does the gentleman from Nebraska, Mr. Terry? Okay. The gentleman from Texas, Mr. Green?

Mr. GREEN. Mr. Chairman, I just am glad we are considering this bill, and I will waive and ask for extra time on questions.

Chairman BARTON. Okay. Does the distinguished vice-chairman, Mr. Pickering, wish to make an opening statement?

Mr. PICKERING. I just wish you a good morning, and I will pass.

Chairman BARTON. All right.

The gentlelady from California, Ms. Solis?

Ms. SOLIS. Yes, I will pass and just include something for the record, and want to also welcome the new members of the Energy and Commerce Committee.

Chairman BARTON. The gentleman from New Jersey, Mr. Burgess?

Mr. BURGESS. For fear of the mute button, I will pass, Mr. Chairman.

Chairman BARTON. Okay. The gentleman from Texas, Mr. Gonzalez?

Mr. GONZALEZ. No, thank you.

Chairman BARTON. The gentleman from Michigan, Mr. Rogers?

Mr. ROGERS. I will waive.

Chairman BARTON. My gosh, we are doing great.

The gentleman from Washington, Mr. Inslee, a new member?

Mr. INSLEE. No, thank you.

Chairman BARTON. The gentleman from Idaho, Mr. Otter?

Mr. OTTER. No.

Chairman BARTON. Okay. The gentlelady from Wisconsin is going to waive. Okay. The gentlelady from North Carolina, Ms. Myrick? Okay. Does the gentleman from Arkansas wish to make an opening statement? Welcome to the committee. Okay. And I do want to tell our new members, we are giving you name tags, so I am—I apologize if we don't have them ready today, but they are on the way.

Let us see, the gentleman from Pennsylvania, Mr. Murphy?

Mr. MURPHY. I would like to waive, but since this is my opportunity, and in lieu of a nametag, I would just like to mention a few things. This is the first hearing I am attending, and I am grateful to be a member of this committee now.

Chairman BARTON. The gentleman is recognized for 3 minutes.

Mr. MURPHY. Thank you.

I am grateful to be a member of this committee because of issues such as this. Spyware is such an insidious problem in computers where the multibillion-dollar industry of people having systems in their own home have been destroyed by unscrupulous folks. Now these go by many names, and sometimes they even appear to be legitimate systems, but anything that does not allow the owner of their own computer to opt-in fully informed is wrong and should be made illegal. The points have been made earlier, but I know some of them, and being the father of a teenage daughter, I see this myself, too. It seems whenever she gets an e-mail from someone, some spyware might be attached to it as well, Gator being one of the more insidious ones, which suddenly find every time I—it is on the computer, I would have to work to get it off. And that is wrong that companies are using this, that they are able to download information, they are able to put software on computers, and I am grateful that this committee is moving forward on that.

With that being said, I enthusiastically look forward to the remainder of this hearing.

Thank you, Mr. Chairman.

Chairman BARTON. We thank the gentleman from Pennsylvania.

Does the gentleman from Texas, Dr. Burgess, wish to make an opening statement? Mr. Whitfield of Kentucky, do you wish to make an opening statement? Mr. Whitfield waives.

Seeing no other member present, the Chair would ask unanimous consent that all members not present have the regular number of days to enter a written statement into the record. Without objection, so ordered.

[Additional statements submitted for the record follow:]

PREPARED STATEMENT OF HON. PAUL E. GILLMOR, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO

I thank the Chairman for holding this hearing today, kicking off another successful and productive year for our panel.

With regard to H.R. 29, the SPY ACT, I am happy to add my name as a cosponsor this year, which is identical to the measure that the full House approved overwhelmingly last October.

This legislation represents yet another effort by our committee to protect personal privacy, as it aims to curb computer programs that literally spy on its users. "Spyware" can easily high-jack our computers by downloading unrelated software when we simply click on a banner or pop-up ad. It then has the ability to silently record our every click, keystroke, and Internet search, gathering information such as passwords and credit card numbers. I particularly appreciate the provision in the SPY Act providing for a prominent "opt-in" for consumers prior to downloading any monitoring software onto that user's computer.

I look forward to the input of our well-balanced panel of witnesses, welcome the new members of the Energy and Commerce Committee, and remain hopeful that H.R. 29 will soon be considered for swift approval in the 109th Congress.

Again, I thank the Chairman and yield back the remainder of my time.

PREPARED STATEMENT OF HON. CHARLIE NORWOOD, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF GEORGIA

Thank you Mr. Chairman.

Before I start my statement I'd like to extend a warm welcome to the new members of the committee. I look forward to working with all of you throughout this Congress.

Mr. Chairman, I'd like to thank you for holding this hearing today on H.R. 29, the SPY Act. This is a very clear-cut consumer privacy issue, one that I think is vital that we address for our constituents back home.

Last year, Ms. Bono's SPY Act passed overwhelmingly in the House, but got tangled up in the other body. As we all know, "spyware" in its most intrusive form can invade a constituent's computer, steal their social security number and credit card information. On the other hand, spyware can also provide legitimate businesses with a vital tool for increasingly productivity.

Striking a balance is vital for the SPY Act to succeed. I want to make sure the citizens of the Ninth District of Georgia are protected from fraud, but I do not want to overburden businesses with lengthy federal regulations. I believe H.R. 29 strikes this balance. That being said, I look forward to our witnesses' testimony today to weigh in their opinions.

Thank you Mr. Chairman, I yield back.

PREPARED STATEMENT OF HON. MARY BONO, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Good morning, and thank you Mr. Chairman for holding this hearing today and for your continued interest and support in Cybersecurity. I would like to thank Congressman Towns for his support and efforts on this bill. He has been a champion of this issue and legislation from the beginning. I would also like to thank Ranking Member Congressman Dingell for his continued leadership on this issue, as well as Congressman Stearns and Congresswoman Schakowsky for their hard work to make this legislation a reality. I am hopeful that the testimony today from our witnesses is instrumental in helping the Committee formulate effective legislation on the issue of Spyware. Cybersecurity and the protection of personal data of consumers is a very real issue that warrants the attention and action of government, businesses, and consumers alike.

There are many things that consumers can do to protect themselves. Anti-virus software and patches are regularly available for downloading and updating. Moreover, one should always be cautious while downloading software from unknown or un-trusted sources. Consumers should avoid opening e-mails from strangers and should be hesitant to disclose personally identifiable information over non-secure sites. However, the methods of hackers are evolving into misrepresentations to the consumer and tricking them into divulging their private information. Moreover, the methods and practices of these hackers and spyware users are getting past expert computer users and the most diligent anti-spyware customers—reflecting the true vulnerability of all computer users.

Due to the overwhelming support (399-1) of H.R. 2929 last year, I reintroduced H.R. 29, "The Securely Protect Yourself Against Cyber Trespass Act ("the SPY Act")." This bill aims to empower consumers to help safeguard them from bad actors. Unfortunately, consumers regularly and unknowingly download software programs that have the ability to track their every move. Consumers are sometimes

informed when they download such software. However, the notice is often buried in multi-thousand word documents that are filled with technical terms, and legalese that would confuse even a high tech expert. Many spyware programs are surreptitiously designed to shut off any anti-virus or firewall software program it detects.

The SPY Act would help prevent Internet spying by requiring spyware entities to inform computer users of the presence of such software, the nature of spyware, and its intended function. Moreover, before downloading such software, spyware companies would first have to obtain permission from the computer user.

This is a very basic concept. The PC has become our new town square and global marketplace as well as our private database. If a consumer downloads software that can monitor the information shared during transactions, for the sake of the consumer as well as e-commerce, it is imperative that the consumer be informed of whom he or she is inviting into their computer and what he or she is capable of doing with their private information. After being informed, the consumer should have the chance to decide whether to continue with the download or reject the presence of such software. In short, consumers should be put in a position where they can make an informed choice about their private personal information.

Once installed on computers, some spyware programs, like viruses, become imbedded among code for other programs and affect how those programs function on the user's computer. Additionally, spyware is becoming more and more difficult to detect and remove. Usually, such programs are bundled with another unrelated application and cannot be easily removed, even after the unrelated application has been removed.

Moreover, the advertisements may not always be forthcoming. Many times, spyware entities contract with companies to post advertisements and in turn, post such advertisements on the websites of competitors. The result is confusion. In other words, while visiting the website for Company A, you may be browsing to purchase a product. However, while browsing a pop up link may appear informing you of a great sale. Under the impression that you are looking at a link for Company A, you may purchase the product, all the while uninformed that the product was purchased via a pop-up link from Company B.

According to a recent study, many problems with computer performance can be linked in some way to spyware and its applications. Additionally, some computers have several hundred spyware advertising applications running, which inevitably slow down computers and can cause lockups. Some spyware can literally shut down your computer forcing the user to spend time and money getting their computer to function normally again. If you have spyware on your computer, you most likely are getting more pop-up advertisements than you would if you had no such software on your computer. I know the effects of spyware from personal experience as my daughter's computer has been completely shut down by this software.

All of these consumer disadvantages can be decreased or eliminated if disclosures surrounding spyware are required and enforced. If consumers are informed about spyware, chances are they may not choose to download the software. Upon choosing not to download spyware: consumer's computers will run more efficiently; their anti-virus programs and firewalls will function better; they can decide which information to share and not share; and consumers will not be deceived into buying a product or service from unknown entities.

Since the introduction of H.R. 29, I have had the opportunity to speak with many different sectors of the technology industry and retail businesses that operate on the Internet. Through these discussions, I have received meaningful feedback. I am currently working on refining H.R. 29. Some of these refinements include the following—

- Prohibiting the unauthorized downloading of spyware without prohibiting the downloading of beneficial programs such as anti-virus software;
- Prohibiting the unauthorized use of spyware without prohibiting authorized uses and the use of cookies;
- Requiring spyware programs to be easily removable after they have been downloaded;
- Ensuring that the "clear and conspicuous" notices required in H.R. 29 are very clear; and
- Preventing deceptive advertisements that are facilitated through spyware.

I look forward to continually working with the technology industry in order to produce a bill that protects consumers and legitimate uses of that information. Government and private enterprise must team up as one because the war against spyware cannot be done alone.

Thank you, and I look forward to the testimony of the witnesses on this issue.

PREPARED STATEMENT OF HON. GENE GREEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Thank you Chairman Barton and Ranking Member Dingell for your leadership on this issue. Our colleagues, Representatives Bono and Towns did a great job moving this legislation through this committee and the House with overwhelming bi-partisan support. I hope in this Congress, we see this bill sent to the President and enacted.

As a co-sponsor of the Anti-SPAM bill with our colleague Heather Wilson, I understand the importance of this issue. In fact, earlier this month, in my home state of Texas, the Attorney General has filed the first state suit against a SPAM operation which is listed in the top five SPAM operations in the world. Thanks to the Anti-SPAM legislation this committee passed, each person behind this operation now faces fines of up to $2 million each.

Given our success with Anti-SPAM legislation, I believe we are on the right track with the Spyware legislation.

We live in an age when technological breakthroughs bring us better, more efficient lives. However, these breakthroughs also entice people to take advantage of others for personal and financial gain.

Congress needs to address these types of issues quickly because as we all know, the fast pace of technological growth will always bring with it new issues for Congress.

During our experience with the Anti-SPAM bill, we all came to an understanding that technology itself is not the problem—it is the way some people and businesses use technology that is harmful to consumers.

We were able to move this legislation quickly last Congress and I hope we are able to address any issues that may help this Committee send an even better bill to the Floor to ensure passage in the Senate.

I think this legislation as it stands is strong. With the commitment Congresswoman Bono and Congressman Towns have made to make this legislation fair and enforceable, I'm confident we can see this bill become a law in the near future.

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

PREPARED STATEMENT OF HON. HILDA L. SOLIS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Chairman Barton and Ranking Democrat Dingell, thank you for holding this hearing today. The issue of privacy is one that is important to me. Privacy is one of the civil liberties we have as Americans that makes this nation so special. Too often I hear from my constituents that they fear their privacy is being invaded and they are powerless to defend themselves.

I believe legislation is critical to provide consumers the tools they need to regain their right to privacy. Last year I supported H.R. 2929 because I felt it provided the resources consumers needed. It is good to be supporting legislation that would not only strengthen security but also strengthen privacy—one of America's key civil liberties.

I want to thank Ed Towns, Jan Schakowsky, Mary Bono, Cliff Stearns and others for their leadership on this issue, and I look forward to hearing comments on this legislation in the hopes that it too can help our consumers protect themselves. I look forward to working with my colleagues this year to hopefully take steps to make today's America a better America.

Chairman BARTON. We want to welcome our witness list today. We have Mr. David Baker, who is the Vice President, Law and Public Policy for EarthLink in Atlanta, Georgia. We have Mr. Ira Rubinstein, the Associate General Counsel for Microsoft, who represents them here in Washington, DC. We have Mr. Howard Schmidt, who is the President and Chief Executive Officer of R&H Security Consulting in Issaquah, Washington. And we have Mr. Ari Schwartz, who is the Associate Director for the Center for Democracy and Technology here in Washington, DC. Gentlemen, welcome to the committee. Your statements are in the record in their entirety. We are going to start with Mr. Baker and give each of you 7 minutes to expand upon your written statement.

Welcome to the committee, Mr. Baker.

STATEMENTS OF DAVID N. BAKER, VICE PRESIDENT, LAW AND PUBLIC POLICY, EARTHLINK, INC.; IRA RUBINSTEIN, ASSOCIATE GENERAL COUNSEL, MICROSOFT CORPORATION; HOWARD A. SCHMIDT, PRESIDENT AND CHIEF EXECUTIVE OFFICER, R&H SECURITY CONSULTING; AND ARI SCHWARTZ, ASSOCIATE DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. BAKER. Thank you.

Chairman Barton, 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 one of the Nation's largest Internet service providers, serving over 5 million customers nationwide with broadband, dial-up, web hosting, and wireless Internet services. EarthLink is always striving to improve its customers' online experience. To that end, we appreciate the efforts of this committee to combat the growing problem of spyware.

We have reached a point in time where spyware has equaled, if not surpassed, spam as the biggest problem facing Internet users. Spyware compromises consumers' online experience and security. As the Wall Street Journal noted last April, "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." Like spam, we must fight spyware on several fronts. Legislation, enforcement, customer education, and technology solutions are all needed to combat this growing threat. We spoke here last year in support of H.R. 2929, the SPY ACT, which passed the House by a 399-1 margin last October. Similarly, we appear here today in support of the efforts of Congresswoman Bono, Congressman Towns, their cosponsors, and this committee to reintroduce this year's H.R. 29, the SPY ACT. Prohibiting the installation of software without a user's 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.

Spyware comes in several different forms, each presenting unique threats. Adware is advertising-supported software that displays pop-up advertisements whenever the program is running. Although it is seemingly harmless, adware can install components on your computer that track personal information.

Adware cookies are pieces of software that websites store on your hard drive when you visit a site. Some cookies save you time, for example, when you check a box for a website to remember your password on your computer, but some adware cookies store personal information, like your surfing habits, user names, and passwords, and areas of interests and share that information with other websites.

System monitors can capture virtually everything you do on your computer, from keystrokes, e-mails, and chat room dialog to which sites you visit and which programs you run. System monitors usu-

ally run in the background so that you don't know you are being watched. The information gathered by a system monitor is stored on your computer in an encrypted log file for later retrieval.

Trojan horses are malicious programs designed to steal or encode computer data and to destroy systems. Some Trojan horses, called RATs, Remote Administration Tools, give attackers unrestricted access to your computer whenever you are online. Trojan horses are distributed as e-mail attachments or they can be bundled with other software programs.

As a leading Internet provider, EarthLink is on the front lines in combating spyware. EarthLink makes available to both its customers and to the general public technology solutions, such as EarthLink Spy Audit powered by Webroot. Spy Audit is a free service that allows an online user to quickly examine his or her computer to detect spyware. A free download of Spy Audit is available on EarthLink's website. EarthLink members also have access to EarthLink Spyware Blocker, which disables all common forms of spyware, including adware, system monitors, keystroke loggers, and Trojans. EarthLink Spyware Blocker is available for free to EarthLink members as a part of Total Access 2005, our Internet access software. In addition to Spyware Blocker, Total Access 2005 includes a suite of protection tools, such as Spam Blocker, Pop-Up Blocker, Scam Blocker, which blocks phisher sites, Virus Blocker, and Parental Controls.

As indicated in the attachment to my testimony, over 3.2 million Spy Audit scans performed in the first 3 quarters of 2004 found over 83 million instances of spyware. This represents an average of 26 spyware programs per scanned PC. While most of these installations were relatively harmless adware and adware cookies, the scans revealed over 1 million installations of much more serious system monitors and Trojans.

Spyware is thus a growing problem that demands the attention of Congress, enforcement agencies, consumers, and industry alike. Through the efforts of Congress to introduce legislation like the SPY ACT, enforcement actions by the FTC and other agencies, 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.

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

PREPARED STATEMENT OF DAVID N. BAKER, VICE PRESIDENT, LAW AND 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 one of the nation's largest Internet Service Providers (ISPs), serving over 5 million customers nationwide with broadband (DSL, cable and satellite), dial-up, web hosting and wireless Internet services. EarthLink is always striving to improve its customers' online experience. To that end, we appreciate the efforts of this committee to combat the growing problem of spyware.

SPYWARE: A GROWING THREAT

We have reached a point in time where spyware has equaled if not surpassed spam as the biggest problem facing Internet users. Spyware compromises consumers' online experience and security. As the Wall Street Journal noted even last year, "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." "What's That Sneaking Into Your Computer?" Wall Street Journal, April 26, 2004.

Like spam, we must fight spyware on several fronts. Legislation, enforcement, customer education and technology solutions are all needed to combat this growing threat. We spoke here last April in support of H.R. 2929, the Safeguard Against Privacy Invasions (SPI) Act, which became the Securely Protect Yourself Against Cyber Trespass Act (SPY ACT) and which passed the House by a 399-1 margin last October. Similarly, we appear hear today in support of the efforts of Congresswoman Bono, her co-sponsors and this Committee to re-introduce this year's H.R. 29 the SPY ACT. Prohibiting the installation of software without a user's 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.

VARIOUS FORMS OF SPYWARE

Spyware comes in several different forms, each presenting unique threats:

Adware is advertising-supported software that displays pop-up advertisements whenever the program is running. Often the software is available online for free, and the advertisements create revenue for the company. Although it's seemingly harmless (aside from the intrusiveness and annoyance of pop-up ads), adware can install components onto your computer that track personal information (including your age, sex, location, buying preferences, or surfing habits) for marketing purposes.

Adware cookies are pieces of software that Web sites store on your hard drive when you visit a site. Some cookies exist just to save you time-for example, when you check a box for a Web site to remember your password on your computer. But some sites now deposit adware cookies, which store personal information (like your surfing habits, usernames and passwords, and areas of interest) and share the information with other Web sites. This sharing of information allows marketing firms to create a user profile based on your personal information and sell it to other firms.

System monitors can capture virtually everything you do on your computer, from keystrokes, emails, and chat room dialogue to which sites you visit and which programs you run. System monitors usually run in the background so that you don't know you're being watched. The information gathered by the system monitor is stored on your computer in an encrypted log file for later retrieval. Some programs can even email the log files to other locations. There has been a recent wave of system monitoring tools disguised as email attachments or free software products.

Trojan horses are malicious programs that appear as harmless or desirable applications. Trojan horses are designed to steal or encode computer data, and to destroy your system. Some Trojan horses, called RATs (Remote Administration Tools), give attackers unrestricted access to your computer whenever you're online. The attacker can perform activities like file transfers, adding or deleting files and programs, and controlling your mouse and keyboard. Trojan horses are distributed as email attachments, or they can be bundled with other software programs.

EARTHLINK'S 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 an online user to quickly examine his or her computer to detect spyware. A free download of Spy Audit is available at www.earthlink.net/spyaudit. 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 to EarthLink members as part of Total Access 2005, our Internet access software. See www.earthlink.net/home/software/spyblocker.

In addition to Spyware Blocker, Total Access 2005 includes a suite of protection tools such as spamBlocker, Pop-Up Blocker, Scam Blocker (which blocks phisher sites), Virus Blocker, and Parental Controls.

Over 3.2 million Spy Audit scans performed in the first 3 quarters of 2004 found over 83 million instances of spyware. This represents an average of 26 spyware programs per scanned PC. While most of these installations were relatively harmless

adware and adware cookies, the scans revealed just over 1 million installations of more serious system monitors or Trojans.

CONCLUSION

Spyware is thus a growing problem that demands the attention of Congress, enforcement agencies, consumers and industry alike. Through the efforts of Congress to introduce legislation like the SPY ACT, enforcement actions by the FTC and other agencies, 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.

Chairman BARTON. Thank you, Mr. Baker.

And Mr. Rubinstein, before you speak, we are going to lower the screen in the back, so we can have the TV picture, and it is somewhat noisy. So if you will suspend until we can get the screen down in the back.

We didn't want to interrupt his testimony. So welcome to the committee, Mr. Rubinstein, and your testimony is in record. We give you 7 minutes to expand upon it.

STATEMENT OF IRA RUBINSTEIN

Mr. RUBINSTEIN. Thank you.

Chairman Barton, Ranking Member Dingell, and members of the committee, my name is Ira Rubinstein, and I am an Associate General Counsel at Microsoft. Thank you for the opportunity to share our views on spyware, an issue of which you have been at the forefront. In particular, I want to acknowledge the leadership of Chairman Barton and Ranking Member Dingell, Chairman Stearns and Ranking Member Schakowsky of the Consumer Protection Subcommittee, and Representatives Bono and Towns, the lead sponsors of H.R. 29, the SPY ACT.

This committee has worked tirelessly to draft legislation that targets the bad behavior at the root of the spyware problem, without unnecessarily impacting legitimate software functionality. We support the SPY ACT, and we look forward to working with Congress as the bill moves forward.

Nine months ago, Microsoft testified on spyware before the Consumer Protection Subcommittee. We described a multifaceted approached that included technological development, consumer education, aggressive enforcement, and industry best practices. We also discussed the role of legislation in complementing this strategy. Since then, we have made significant headway in each of these areas. Today, I want to update the committee on that progress and describe how industry and Congress can continue working together to give consumers choice and control.

Spyware is a problem of bad practices, practices that mislead, deceive, or even bully users into downloading unwanted applications. However, new anti-spyware technology is enabling users to fight back. For example, Microsoft recently released a Beta, or test version, of Windows AntiSpyware. This is our first dedicated anti-spyware solution, and it is available for free on www.Microsoft.com/spyware. This tool scans a user's computer, locates spyware, and enables——

Chairman BARTON. Mr. Rubinstein, is your microphone turned on?

Mr. RUBINSTEIN. Yes, it is, sir.

Chairman BARTON. Okay. Could you then place it somewhat closer? We are having some trouble up here hearing you.

Mr. RUBINSTEIN. Yes, I will.

Chairman BARTON. Thank you.

Mr. RUBINSTEIN. This tool scans a user's computer, locates spyware, and enables the user to remove it and undo any damage. It also provides ongoing protection to computers through security checkpoints. These guard against more than 50 separate ways that spyware can be downloaded. If known spyware is detected at these checkpoints, it is blocked. If an unknown program is detected, Windows AntiSpyware informs the user and asks whether the download should proceed. We invite the committee to download the program and would welcome your feedback.

In addition to technological developments, there has been substantial progress in other areas. This progress is attributed to the successful collaboration between government and industry. Consumer education is a good example. Over the past 9 months, through hearings like these, consumers have become more aware of the spyware problem and how they can protect themselves from these threats. Industry has also played an important role. Microsoft's AntiSpyware web site contains updated information that is designed to help consumers to understand, identify, prevent, and remove spyware. The site also includes step-by-step instructions on what consumers can do about spyware and an informative 3-minute video covering the same materials. Many others in the industry are engaged in similar efforts.

Cooperation between the public and private sectors has also led to a successful FTC enforcement action against the spyware publisher. Microsoft actively supported this investigation, and we will continue to work with government and industry partners to go after spyware distributors.

Industry best practices are another part of our anti-spyware strategy. They can serve as a foundation for programs that help identify the good actors. This, in turn, allows users to make more informed decisions about the software they download.

Over the past year, representatives from a broad range of companies have been working to develop and implement a set of best practices, but more needs to be done. Microsoft is dedicated to work with industry in this effort that will help optimize user control.

Federal legislation can be an effective complement to this combination of technology, education, enforcement, and industry best practices. But as we have stressed throughout the legislative progress—process, Congress must proceed cautiously to ensure that such legislation targets the deceptive behavior of spyware publishers and not features or functionalities that have legitimate uses.

Our success in working together to achieve this goal is apparent, and our written testimony sets forth some of the scenarios that could have had unintended consequences, but that the committee has now addressed. As we move forward, we need to make sure that the law does not create disincentives for consumers to use these anti-spyware tools or leave anti-spyware vendors open to legal action for developing and distributing them.

We want to thank the committee, again, for your attention to the spyware problem and for extending Microsoft the invitation to share our ideas and experiences with you, both today and as the process moves forward. We appreciate that the committee solicited further comment from industry on ways the clarify the bill, and we encourage the committee to continue this collaborative process. Microsoft remains committed to supporting legislation that will prevent bad actors from deceiving consumers and destroying their computing experience.

Thank you.

[The prepared statement of Ira Rubinstein follows:]

PREPARED STATEMENT OF IRA RUBINSTEIN, ASSOCIATE GENERAL COUNSEL, MICROSOFT CORPORATION

Chairman Barton, Ranking Member Dingell, and Members of the Committee: My name is Ira Rubinstein and I am an Associate General Counsel at Microsoft Corporation. I want to thank you for the opportunity to share with the Committee Microsoft's views on addressing spyware—an issue on which this Committee has been at the forefront. In particular, I want to thank Chairman Barton and Ranking Member Dingell, Representatives Stearns and Schakowsky, the Chairman and Ranking Member, respectively, of the Commerce, Trade, and Consumer Protection Subcommittee, and Representatives Bono and Towns, the lead Republican and Democrat sponsors of H.R. 29, the SPY ACT. This Committee has worked tirelessly to raise public awareness of the threat posed by spyware, and to draft legislation that is carefully targeted to address the bad behavior at the root of the problem—without unnecessarily impacting legitimate software applications. Microsoft believes the Committee has met this goal: we are therefore pleased to support the SPY ACT in its current form, and we look forward to working with Congress as the bill moves forward.

Nine months ago, my colleague Jeffrey Freidberg, who is the Director of Windows Privacy at Microsoft, testified at a hearing of this Committee's Subcommittee on Commerce, Trade, and Consumer Protection on the nature and nuances of spyware, and provided a slide presentation demonstrating some common tricks used by nefarious spyware publishers to deceive users into downloading unwanted programs. He also described Microsoft's commitment to attacking spyware on several levels—technology, consumer education, industry best practices, and enforcement—and the role of legislation in complementing this strategy. Today, I want to tell you about the progress that has been made in each of these areas over the past nine months, and the ways in which the public and private sectors can continue working together to restore choice and control back where it belongs—in the hands of consumers.

Spyware Remains a Pervasive Problem.

As Chairman Barton aptly recognized at last year's hearing, spyware represents an "unwanted intrusion that is used for purposes that we have not approved, and most of the time without our even knowing it." [1] Purveyors of spyware manipulate computer users through misleading download requests, false icons, and covert practices that trick users or override low security settings in order to install programs that users do not need or want. Unlike legitimate applications, these programs show no respect for users' ability to control their own computers, and they misuse many features that can be an asset with proper disclosure, user authorization, and control. Instead of leading to personalization and better user experiences, these features are manipulated to surreptitiously monitor user activities, hijack home pages, and deliver an unstoppable barrage of pop-up advertisements. In short, spyware is a problem of bad practices—practices that mislead, deceive, or even bully users into downloading unwanted applications.

Spyware continues to be a primary frustration for our customers and industry partners. We receive thousands of calls from customers each month directly related to deceptive software, and we continue to receive reports that suggest such software is at least partially responsible for approximately one-half of all application crashes that our customers report to us. In addition, industry partners have indicated that unwanted and deceptive software remains one of the top support issues they face,

[1] *Spyware: What You Don't Know Can Hurt You: Hearing Before the House Subcomm. on Commerce, Trade, and Consumer Protection of the Comm. on Energy and Commerce,* 108th Cong. 77 (2004) (statement of Chairman Barton, House Comm. of Energy and Commerce).

and we understand that it costs many of the large computer manufacturers millions of dollars per year.

Other studies demonstrate the continued growth of the problem. A study last fall conducted by America Online and the National Cyber Security Alliance found that approximately 80 percent of all users had some form of spyware or adware on their machines, and that the average computer contained 93 spyware or adware components.[2] Perhaps most troubling, 89 percent of respondents whose computers had tested positive were unaware that their systems contained any spyware.[3] Over the past year, we have also seen a rise in a particularly disturbing form of spyware programs—so-called "betrayware." These applications claim to be anti-spyware detection or removal programs, but are in fact spyware; some analysts now estimate that there are more than 130 separate betrayware programs lurking in cyberspace.[4]

The explosion in the volume of spyware, and the accompanying increase in the complexity with which those programs operate and the damage that they do, has had an enormous impact on Microsoft. As we explained last year, 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. Spyware programs have increased our support costs, harmed our reputation and, most importantly, thwarted our efforts to optimize our customers' computing experiences.

Anti-Spyware Tools Are Enabling Consumers To Take Back Control.

Although spyware is becoming more pervasive and complex, the good news is that there have also been enormous strides over the past year in the fight against spyware—particularly with respect to the development of anti-spyware tools that empower users to protect themselves. As one example, in January of this year, Microsoft launched the Beta version of Windows AntiSpyware—Microsoft's first dedicated anti-spyware tool based on technology developed by GIANT Software Company, Inc. Microsoft acquired this technology from GIANT and rapidly developed and distributed the anti-spyware beta because our customers have made clear that spyware represents a major problem to them, and that they want Microsoft to deliver effective solutions as quickly as possible.

Windows AntiSpyware works by scanning a customer's computer to locate spyware and other known deceptive software threats, and then giving users the tools to easily and rapidly remove those programs—as well as to quickly restore certain damage done by these programs. Once the spyware has been removed, the Windows AntiSpyware Scan Scheduler enables the scheduling of regular scans to help users maintain the condition of their computers. Windows AntiSpyware can also be configured to block known spyware and other unwanted software from being installed on the computer in the first place. To do this, the program relies on the worldwide SpyNet™ community, which plays a crucial role in determining which suspicious programs are classified as spyware. A voluntary network of users, SpyNet™ helps uncover new threats quickly to ensure that all users are better protected, and any user can choose to join SpyNet™ and report potential spyware to Microsoft. When new spyware programs are confirmed through SpyNet, their unique digital identifiers, or "signatures," can be automatically downloaded by Windows AntiSpyware, helping to stop these new threats before they gain a foothold.

Windows AntiSpyware also provides continuous protection to computers, establishing security checkpoints to guard against more than 50 separate ways that spyware can be downloaded. These checkpoints are monitored by (1) *Internet agents* that help protect against spyware that makes unauthorized connections to the Internet or changes a computer's Internet settings; (2) *system agents* that guard against spyware that makes unauthorized changes to a computer's non-Internet settings (such as passwords or security levels); and (3) *application agents* that protect against spyware that alters applications (such as modifying browsers or launching unwanted programs). If known spyware is detected at these checkpoints, it will be blocked. If an unknown program is detected, Windows AntiSpyware informs the user and asks whether to let the download proceed.

Another feature of Windows AntiSpyware is its ability to work with the security enhancements in Windows XP Service Pack 2 ("XPSP2"). When Mr. Friedberg testified before the Subcommittee last April, he described a number of ways in which XPSP2 would help block the entry points used by spyware programs by better in-

---

[2] *See* AOL/NCSA Online Safety Study (Oct. 2004), *available at* http://www.staysafeonline.info/news/safety__study__v04.pdf.

[3] *Id.*

[4] *See* Eric L. Howes, *The Spyware Warrior List of Rogue/Suspect Anti-Spyware Products & Web Sites, available at* http://www.spywarewarrior.com/ rogue—anti-spyware.htm.

forming users in advance about the type of software they would be installing. As promised, Microsoft did introduce XPSP2 in 2004, and these enhancements are designed to target the particular tricks that spyware distributors use to surreptitiously install unwanted programs:

- A new pop-up blocker, turned on by default, that reduces a user's exposure to unsolicited downloads;
- A new download blocker that suppresses unsolicited downloads until the user expresses interest;
- 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, and allow users to choose to never install certain types of software; and
- A new policy that restricts a user's ability to directly select "low" security settings.

Beyond Windows AntiSpyware and XPSP2, Microsoft will continue working collaboratively with all of our security partners: developing anti-spyware tools that empower our customers to protect themselves is a top priority. In the short term, we want everyone to run some kind of anti-spyware solution on a regular basis. In the long term, we want to develop and implement solutions so that spyware is no longer a major issue for our customers. This is an ambitious goal that will require cooperation and dedication, but we believe that the acquisition of GIANT and implementation of Windows AntiSpyware and XPSP2 are significant strides toward achieving that result.

Advances in Education, Enforcement, and Industry Standards Are Evident.

Technology is a critical part of the solution to spyware, but it cannot work alone. Heightened consumer education, aggressive law enforcement, and improved industry self-regulation are also important to ending the spyware epidemic. In the nine months since Microsoft last testified on spyware, there have been significant developments in each of these areas.

Consumer Education. A year or two ago, only the most sophisticated users even knew what spyware was, let alone how to stop it. Now spyware is becoming well-known as a critical consumer protection issue. For example, in its first day on the Microsoft home page, our new Windows AntiSpyware site received more than 130,000 clicks—easily a record for a launch on our home page, and an indication of the tremendously increased customer interest in and attention to the spyware problem.

Much of the credit for heightening consumer awareness about spyware should go to Congress—and particularly to this Committee. Through hearings such as this and determined efforts to enact effective anti-spyware legislation, Congress has attracted media attention to the spyware problem, and has helped educate consumers about the importance of the issue and how to protect themselves. Industry should also play a role in consumer education, and the Web site we launched in 2004—www.microsoft.com/spyware—contains information that is specifically designed to help consumers understand, identify, prevent, and remove spyware. We update this site regularly, and it now includes a comprehensive but easy-to-read white paper describing our spyware strategy, as well as public newsgroups on spyware that our security-focused "most valuable professionals" monitor to assist the online community. We want to provide users with clear, current, and trusted resources to help understand, remove, and avoid spyware.

Representative Bono emphasized last year that "it is necessary that we [government and industry] collectively educate consumers about the nature and the threats of spyware," and we agree.[5] Although much work has been done over the past year to educate consumers about spyware, we are committed to continuing to working with you and other industry members in this important effort.

Enforcement of Existing Laws. The use of aggressive enforcement actions against spyware purveyors is another critical part of our approach to the problem. Targeting the most insidious violators would have a significant impact on the amount and type of spyware that is produced and distributed—and would serve as a powerful deterrent to would-be violators.

Last April, we explained to the Subcommittee that enforcement actions were possible under existing law. In October 2004, the Federal Trade Commission demonstrated that this was true, taking the first federal enforcement action and obtaining a temporary restraining order against a major distributor of spyware for unfair and deceptive practices that violated the FTC Act. The defendant in that case, Stanford Wallace (who is also known as the "Spam King"), had developed and installed

[5] *Spyware: What You Don't Know Can Hurt You: Hearing Before the House Subcomm. on Commerce, Trade, and Consumer Protection of the Comm. on Energy and Commerce,* 108th Cong. 6 (2004) (statement of Rep. Bono, House Comm. of Energy and Commerce).

on unsuspecting users' computers code that tracked their Internet behavior, changed home pages and search engines, and launched a stream of pop-up ads. Wallace then went a step further and targeted these users with pop-up advertisements promoting faulty anti-spyware remedies that Wallace sold for approximately $30 each.

Microsoft supported the FTC's investigation in that case, and our Internet Safety Enforcement team is committed to enforcing existing laws against the distributors of spyware. The team investigates spyware threats that are reported by customers or others, working with government and industry partners and using advanced technology to find the sources of these programs. After the investigation, the team either pursues these cases internally or refers them to law enforcement, including the FTC, U.S. Attorneys, and State Attorneys General. And as in the suit against the Spam King, the team also assists law enforcement officials with their spyware investigations. Microsoft believes that the public and private sectors should continue to work together to hold spyware publishers accountable for their unlawful acts, and we look forward to other successful enforcement actions in the future.

Industry Best Practices. Developing a set of industry-wide standards is another piece of our spyware strategy. Such best practices create an incentive for legitimate software publishers to distinguish themselves from bad actors, and can serve as a foundation for programs that certify and label the good actors—which in turn empower users to make informed decisions about the software they download to their computers.

Representatives from a broad range of companies have been working to develop and implement a set of best practices, but more needs to be done. Initial efforts have focused on standards for the installation of software through the Internet—as well as more broadly with respect to the collection and use of personal information, the display of pop-up advertisements, and the form and substance of notice and consent. The overriding goal of these practices is to empower consumers—allowing them to make informed decisions by providing appropriate notice and consent experiences, balancing the need for transparency and detail, and offering appropriate controls. Self-regulatory measures should continue to evolve to account for the complexities and challenges that are a result of the ever-changing nature of technology. Microsoft is committed to working with industry to formulate best practices and believes that these practices can help supplement other efforts.

Targeted Legislation Has a Role To Play.

Microsoft is optimistic that this combination of technology, education, enforcement, and industry standards can effectively combat the spyware problem. And significant progress has been made toward this goal in the past year: technological solutions to empower consumers to protect themselves from spyware are now widely available; consumers are much more educated about the nature and scope of spyware; a successful enforcement action has been taken against a spyware publisher under existing law; and legitimate industry practices are becoming better and more consistent.

Federal legislation can be an effective complement to this strategy, providing an additional layer of protection for consumers and another tool for enforcement officials. As we stressed at the beginning of this process, however, Congress must proceed cautiously to ensure that such legislation targets the deceptive behavior of spyware publishers—and not features or functionalities that have substantial legitimate uses. This distinction is critical to avoid imposing unworkable requirements on legitimate applications and adversely affecting legions of computer users.

The Proposed Legislation Has Improved Dramatically.

When we last testified, we offered some scenarios in which well-intended legislation could have unfortunate and unintended consequences. As you know, we were concerned that initial drafts of anti-spyware legislation contained provisions that might compromise specific functionalities rather than target the bad practices at the core of the spyware problem. We have been extremely pleased, however, at the willingness of Representatives Bono and Towns and other members of this Committee to work with us and others in the private sector to create a bill that captures the bad actors without unnecessarily impeding the good ones. Representative Towns recognized this when the SPY ACT was brought to the House floor last year, noting that "any time we legislate on highly technical matters, there is always a danger in stifling innovation or making the use of legitimate software too burdensome. It is a very difficult tightrope to walk, but I think we have done an excellent job in walking that line."[6] That we successfully worked together to achieve this balance is apparent when we re-examine those scenarios we raised last April.

[6] 150 Cong. Rec. H8085 (daily ed. Oct. 5, 2004) (statement of Rep. Towns).

Disruptive User Experience. As we explained then, many legitimate software programs contain an information-gathering functionality that these programs need in order to perform properly. These include 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.

The current version of the SPY ACT understands these issues, and takes steps to safeguard the user experience. In particular, the bill allows notices to consumers to be tailored to take into account different scenarios. It also contains important exceptions for critical functionalities—such as security procedures and authentication checks—and recognizes circumstances where information-sharing is driven by the user. These revisions help the legislation target bad actors without impeding legitimate applications.

Compromised Consent Experience. We were also concerned about "one size fits all" notice and consent requirements, which may not give users sufficient context to make informed decisions. For example, requiring notice and consent at the time of installation ignored 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. Presenting the notice and choice experience for Windows Error Reporting at the time Windows is first installed, in contrast, would lack this critical context.

As a result of cooperation between Congress and industry, the current version of the bill allows for "just in time" consent. This is an important inclusion that empowers users by providing them with notice and requiring choice at the time most appropriate to making an informed decision.

Unrealistic Uninstall Requirements. Finally, we were concerned about provisions in the bill that required standardized uninstall practices for all software, which we feared 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 compromise the security of the system, such as backing out security upgrades or removing critical services.

Here again, the Committee has been responsive to industry concerns, and the bill has been modified to provide legitimate developers with the flexibility necessary to avoid the types of problems outlined above. We look forward to continuing to work with the Committee to ensure that all appropriate uninstall scenarios are adequately addressed.

Legislation Must Be Forward-Thinking.

As Chairman Barton rightly recognized when bringing the SPY ACT to the House floor last term, "technological development moves quickly, much faster than the regulatory or legislative process."[7] We praise the Chairman for his hard work to move the SPY ACT through the legislative process so we can rapidly get additional tools in the hands of regulators to fight this burgeoning threat. But spyware is a relatively new problem, and the list of acts prohibited by the bill today might not capture every practice used by bad actors tomorrow. We and others in the industry are working to develop and implement new and better anti-spyware tools that will empower consumers to make more informed choices with respect to their computers. We need to make sure that the law does not create disincentives for consumers to use these tools, or for companies to develop and distribute them.

Congress recognized the importance of enabling consumers to take advantage of technological tools in addressing spam. In that context, Congress worked to clarify that merely because a message is not unlawful under federal law does not mean that consumers are in any way precluded from using technology to block the mes-

[7] 150 Cong. Rec. H8080-81 (daily ed. Oct. 5, 2004) (statement of Rep. Barton).

sage. Similarly, with respect to spyware, simply because a software program complies with the SPY ACT should not prohibit consumers from choosing whether to download it, nor should it leave vendors of anti-spyware tools open to legal action for providing tools that enable consumers to make these choices. We think it is self-evident that the SPY ACT should support the creation of such tools and not provide disincentives for the development of ever more powerful anti-spyware technologies. We look forward to working with Congress to ensure that the legislation achieves its aims of empowering consumers to maintain control over their computer systems and protect themselves as they see fit.

We want to thank the Committee once again for your attention to the spyware problem and for extending Microsoft an invitation to share our ideas and experiences with you—both today and as this process moves forward. By continuing to attack the problem on several levels—consumer education, technology solutions, industry best practices, aggressive enforcement, and targeted legislation—we believe we can thwart the efforts of those who produce and distribute spyware. Microsoft remains committed to working with you to prevent bad actors from deceiving consumers and destroying their computing experience.

Mr. STEARNS [presiding]. Thank you.

Mr. Schmidt?

STATEMENT OF HOWARD A. SCHMIDT

Mr. SCHMIDT. Good morning, Mr. Chairman.

Mr. STEARNS. Good morning.

Mr. SCHMIDT. Members of the committee, my name is Howard Schmidt. I am the President and CEO of R&H Security Consulting. Over the past 20 years, I have served as a computer crime investigator with the Chandler, Arizona Police Department. I left the FBI's Computer Exploitation Team for the National Drug Intelligence Center at Johnstown, Pennsylvania. I served as the Director of Computer Crime and Information Warfare at the Air Force Office Special Investigations. I have been the Chief Security Officer of Microsoft and eBay. And in the aftermath of September 11, I was appointed by President Bush as the Vice-Chairman of the President's Critical Infrastructure Protection Board and Special Advisor for Siberia Security.

I, to this day, continue to serve, as the privilege, on the U.S. Army Reserves as a computer crime investigator. And I thought I had seen it all until I have seen the effects of what happens with spyware today. And I thank you for the opportunity to share with you my perspective on the impact, an issue that the committee has shown great leadership in working tirelessly to raise awareness and—of a potential threat.

In previous testimony, I have talked about the impact of cybersecurity in our day-to-day lives and the protection of critical infrastructure. Today, I would like to tell you why the threats posed by spyware threaten more than just our privacy and protection of personal information, but also speak briefly as to the progress that market forces and the private sector have made in the past year. It has been proven time and time again that by the public and private sectors working together to protect innovation as well as to improve end user protection.

As Chairman Barton discussed in previous hearings, spyware represents an intrusion into our day-to-day computer experience without our knowledge. But I would like to focus my comments into two specific areas, the end user/consumer area as well as the enterprise.

As some of the members have stated, I got to see firsthand with my own family members the impact that this has. My son is a computer crime detective in Arizona. My wife teaches computer forensics in Wisconsin to law enforcement, but that is sort of where the end of the technology expertise ends in my family. My brother-in-law in Wisconsin, who is a great carpenter, wound up finding his computer totally unusable after being hijacked—his browser was hijacked by a system that even programs designed to remove that specific system were unable to do so, which we had to completely rebuild the system. On the other end of the spectrum, my 88-year-old father lives in Florida and uses the Internet for entertainment, communication with friends around the country, and digital photography. Within a few moments of buying—a few days after buying it, the new computer was akin to a 15-year-old computer system.

To this, we have seen industry respond rapidly to deal with the intrusiveness of spyware. We started putting out pop-up blockers, making them available for free, and anti-virus vendors started to include spyware technology into the security suites. As Mr. Rubinstein mentioned, Microsoft recently launched a product that, once again, helps deal with these products.

But as we continue to work on the problem of spyware, we need to remember that much of the benefits we derive from online experience is based on the interactive nature of the Internet. In the early days of computing, people used computers to do things, and to this day, in many instances, computers interact with other computers, so consequently, we want to make sure we don't disrupt, and this committee has paid a great deal of attention to impacting that interaction on our behalf.

One of the things that we discussed were the convergence of various technologies, voice-over IP, telecommunications, and computers. One of the things we have also seen, though, is the convergence of the spyware in the more nefarious aspects of it, including tools that enable systems to be hacked, identity theft, keystroke loggers, and robots, which in turn take over computer systems and use those computers to attack other computer systems through installation of spyware.

While the vast majority of these acts are covered under provisions such as Title 18, Title 5, Electronic Communications Privacy Act, Computer Fraud and Abuse Act, this particular bill, H.R. 29, closes an important gap that we don't see in some of the other things, and it targets a set of behaviors, not specific technologies. It should continue to improve and protect the interactive software used for positive purposes while indeed holding those accountable for the nefarious acts.

There are four major areas, though, that I think are very important when we combat those areas and the many areas of cybersecurity. First, the use of technology and market forces are the strongest potential solution when it comes to dealing with online threats. Thanks to the freely online anti-spyware software, including the new Microsoft product, my father's system, as I have cited a moment ago, was free and hopefully will stay that way for a long time.

Second, the efforts of education and awareness go a long way in informing users what capabilities they have, whether it is Internet phishing threats, Trojans, or spyware, an educated and informed public is a vital weapon for protection of these things.

Third, companies, even competitors are working very closely together to identify new threats, share information with each other, and publish updates to deal with the new threats faster than ever in the past. As a matter of fact, many of the industry leaders are now working together to deal with the factor of two-factor authentication, basically something akin to an ATM card where we can better protect ourselves as well.

And fourthly, is the—as with many other issues harming society, technology, education, and information are not going to be 100 percent solution. To that end, we need to have penalties and trained, equipped, and staffed law environment personnel to enforce these penalties. And while our online safety continues to improve day-by-day, hour-by-hour, this committee's work is crucial to help us get close to that 100-percent level.

The provisions of the SPY ACT should continue to encourage companies to develop and distribute ever more effective and powerful anti-spyware and security technologies, and I look forward to our continued great working relationship with Congress to ensure that the legislation achieves its aims of protecting and empowering consumers in order to protect themselves in the situation to fit them.

I would like to also thank the committee for their continued leadership and attention to this problem and for inviting me to appear before this committee and talk about this issue. I would like to thank you for the ability and look forward to any questions you might have.

Thank you.

[The prepared statement of Howard A. Schmidt follows:]

PREPARED STATEMENT OF HOWARD A. SCHMIDT, PRESIDENT AND CEO, R&H SECURITY CONSULTING LLC

Chairman Barton, Ranking Member Dingell, and Members of the Committee: My name is Howard A. Schmidt and I am President & CEO of R & H Security Consulting LLC. Over the past 20 years I have served as a Computer Crime Investigator, with the Chandler Arizona Police Department, led the computer exploitation team for the FBI at the National Drug Intelligence Center as well as the Director of Computer Crime and Information Warfare at Air Force Office Special Investigations. I have also been the Chief Security Officer for the Microsoft Corporation and Chief Information Security Officer and Chief Security Strategist for eBay Inc. In the aftermath of 9/11, I was appointed by President Bush as the Vice Chairman of the President's Critical Infrastructure Protection Board and Special Advisor for Cyber Security.

I want to thank you for the opportunity to share with the Committee my perspective on the impact of Spyware—an issue on which this Committee has shown great leadership by working tirelessly to raise public awareness of the potential threat posed by Spyware and by drafting legislation that is carefully targeted to address the bad behavior at the root of the problem, without unnecessarily impacting legitimate software applications. As citizens, we owe a debt of gratitude to Chairman Barton, Representatives Stearns and Schakowsky, the Chairman and Ranking Member, respectively, of the Commerce, Trade, and Consumer Protection Subcommittee, and Representatives Bono and Towns, the lead Republican and Democrat sponsors of H.R. 29, the SPY ACT. Your willingness to work closely with the private and public sector makes your contribution to this issue even more valuable.

During my previous testimony before House Committees, I have discussed the implications of cyber security on our day to day lives and the protection of critical in-

frastructure. Today, I would like to tell you why the threats proposed by Spyware threaten more than just our privacy and protection of personal information, but also speak briefly as to the progress that market forces and the private sector have made in the past year. It has been proven time and time again, the tremendous value that results when the public and private sectors work together to protect innovation as well as to improve end user protection.

A. SPYWARE CONTINUES TO BE A THREAT TO CYBER SECURITY.

As Chairman Barton discussed in the previous hearing, Spyware represents an intrusion into our day-to-day computing experience without our knowledge. I would like to focus my testimony in two very similar areas, the "end user/consumer" and the enterprise. Other witnesses in previous testimony, as well as today's testimony, have described what Spyware is and some of it's effects, so I will not delve into what Spyware is and how it works again I do not have to go much further then my own family to see first hand the impact Spyware has on the online experience. While my son is a computer crime detective and my wife teaches computer forensics to law enforcement, the technology expertise stops there. My first example was when my brother-in-law was not able to use his computer for anything because a piece of Spyware had hijacked his browser. Normally it would have been just a matter of resetting the "home page" to the page one would prefer, but this piece of Spyware was so invasive that even using programs specifically designed to remove this application did not function and eventually resulted in his system not functioning at all. He had to send the computer to me in another state and I had to rebuild the entire system.

The second personal example is the PC of my 88 year old father, who uses the PC and the internet for daily entertainment, communications with friends and digital photography. Within a short period of time of him purchasing his new computer, it went from being a high-speed piece of technology to something akin to a 15-year-old computer running so slow it was almost useless. I am sure that these examples are nothing new to many of us in the IT/Security business, but to "normal" users this is very troubling.

To deal with this, industry, using market forces, has responded rapidly to deal with the intrusiveness of Spyware. It started with pop-up blockers being made available for free and then anti-virus vendors started to include anti-Spyware technology into their "security suites." We now have many "toolbars" that have built in pop-up and spy protection. Recently, Microsoft has launched a Spyware product that is in beta form that shows tremendous promise in providing a technology solution to dealing with a large part of the problem.

As we continue to work on the problem of Spyware, we need to remember that much of the benefits we derive from the online experience is based on the interactive nature of the internet. In the early days of internet use, people interacted with computers. However, in the recent past it has become more of an issue of computers interacting with other computers on behalf of people. Although there are those that would exploit computer-to-computer interaction, we should be very sensitive as to not disrupt the legitimate interactive nature of computers acting on behalf of people.

The key difference, as this Committee has learned by working well with the private sector, between good and bad software is not the means by which it is distributed, but the intent and the behavior of the software. As we move towards a computing environment where we develop self-healing, self-repairing, and self-configuring computers, we must ensure the need to, without end-user intervention, have the ability to download upgrades, security fixes, and protective software. Clearly this type of software installation should not and would not fit into the category as Spyware. A classic example is the use of anti-fraud/id theft software updates, these installations are very important to the integrity of the experience on the internet., The concern that many of us have is when the software is introduced in a deceptive manner and performs functions that are annoying or harmful and difficult, if not impossible, to remove.

At the same time that we are discussing the benefits of convergence of modern day technology, there is also a negative convergence of "traditional" hacking, identity theft, key loggers, and "bots" being installed using what we traditionally call Spyware.

While the vast majority of these acts are covered by provisions of Title 18, Title 5, Electronic Communications Privacy Act (ECPA), Computer Fraud and Abuse Act, the FTC's existing authority to pursue unfair or deceptive trade practices, or international law, H.R. 29, the SPY Act, makes an important contribution to supplementing these laws, and I believe will be successful to the extent that it tar-

gets a set of behaviors and not a class of technology. This bill should continue to protect interactive software that is used for positive purposes including where the users have agreed to an end user license agreements (EULA) and understands what their choices are. In short, the end users should be empowered to make their own choices on how they interact with software applications as "one size does not fit all." As many of us said when dealing with many issues of cyber security, we agree that there are four major steps that must be taken to protect end users.

First, the uses of technology and market forces are the strongest potential solution when it comes to dealing with online threats. As I testified earlier, industry has developed a number of technologies to combat not only Spyware but other threats. Industry's efforts are to be commended and these efforts work for the vast majority of the routine cases we face today. Thanks to freely available anti-Spyware software, including the new Microsoft anti-Spyware beta application, my father's computer is now Spyware free and all indications suggest that it will stay that way.

Second, the education and awareness of ALL users is vital to reducing problems associated with many of the internet threats, whether it is "Phishing," virus and Trojans or Spyware, an educated and informed public is one of the best weapons. Many companies have created "Security Centers" on their web sites to better educate their users as to how protect their computers and their privacy. The National Cyber Security Alliance (NCSA) has consumer tips on its website http://www.stafesafeonline.info. Additional information can be found at http://www.personalfirewallday.org, which provides information for users. The FTC has been a leader in the awareness and education about online security.

Third, companies, even competitors, are working closely together to identify new threats, share information with each other and publish updates to deal with new threats faster than ever in the past. Online companies now are providing free anti-virus services, pop up blockers, and anti-Spyware applications to their customers. Additionally, many of the industry leaders in identity management such as RSA, Verisign, Entrust and Geotrust are providing tools to improve 2 factor authentication to protect privacy and identity. The National Cyber Security Partnership has brought together leaders in this space across various sectors to better coordinate and publicize the industry and government accomplishments.

Fourth, as with many other issues harming society, technology, education and information are not 100% effective in solving problems To that end, the need to have penalties and trained, equipped and staffed law enforcement personnel to enforce those penalties are essential. While online safety continues to improve day-by-day, hour-by-hour the work of this Committee is beneficial to help us get closer to the 100% level.

The provisions of the SPY ACT should continue to encourage companies to develop and distribute ever more effective and powerful anti-Spyware and security technologies. I look forward to continuing our great working relationship with Congress to ensure that the legislation achieves its aims of protecting and empowering consumers to control their computer systems and to exercise valuable protective measures which fit their situation.

I again would like to thank the Committee for your leadership and attention to the Spyware problem and for extending the invitation for me to appear before you to share my experiences with you today and as in the future as this process evolves. Cyber security has always and always will employed using a "layered defense" perspective. By working with this body, technology companies, law enforcement agencies, and diplomatic leaders, I believe we can continue to reduce the impact that bad actors have on our online experience and we can continue to strengthen national security, public safety, and economic advancements, while providing for a rich and robust online experience for us all.

I thank you again for the ability to appear here before you today and I look forward to any questions that you may have.

Mr. STEARNS. I thank the gentleman.

Mr. Schwartz, welcome.

STATEMENT OF ARI SCHWARTZ

Mr. SCHWARTZ. Chairman Stearns, Ranking Member Schakowsky, members of the committee, thank you very much for having CDT testify today.

Since the Center for Democracy and Technology last testified on this issue in front of the Consumer Protection Subcommittee in April of last year, the spyware problem has only gotten worse. Just

this week, a study was released that showed that ⅔ of information technology managers now consider spyware to be the biggest threat to network security.

On a personal note, following the holiday season, I can count myself among the tens of thousands of technically—consumers and computer professionals, and from what we have heard, members of this committee who have tried to help a family member or friend fix a computer that has been plagued by spyware. And in my case, it was my father-in-law. I also came to the conclusion that it would be better to buy a new computer and reformat the hard drive than to continue to try and remove the spyware through the existing tools that were supposed to be able to remove the software, as Mr. Schmidt had suggested in his case.

Over a year ago, CDT asked consumers to send us complaints about specific spyware programs so we can investigate them more fully. We now receive so many complaints that we have had to create a prioritizing system in order to try and figure out which ones to prioritize and even which ones to read.

Fortunately, there is also some positive news. On the technology front, companies such as EarthLink and American Online and Microsoft, as we have heard, have begun to distribute anti-spyware tools more actively. The case that CDT brought to the Federal Trade Commission against spyware purveyor Seismic Entertainment last February has come to trial in New Hampshire. This is the first FTC case against a spyware company. The Seismic case highlights the growing complexity of a marketplace that allows mainstream companies to fund illegal activities through a maze of distributors and affiliates. As I document in my written testimony, the relationships are usually so complex that the companies involved do not know more than one player in what becomes a six or seven-level chain of distributors and affiliates.

CDT sees three major areas where action is necessary to stem the disturbing trends for the loss of control and transparency for Internet users in the environment that we now face. First, it is clear that we need stronger enforcement of existing law. CDT brought the Seismic case in February to the FTC's attention. The FTC took action in October. And court proceedings continue through today. If each case takes such a singular focus over such a long period of time, the enforcement will not be able to serve as a real deterrent in this area.

Second, we need even better consumer education, industry self-regulation, and improved technologies to give consumers real control. We have only seen the beginning of what industry can do to help solve this problem on their own.

Last, CDT strongly believes that many of the privacy concerns of spyware, some of which fall out of the scope of current legal protections, could be clearly addressed with an online privacy law. As members of this committee know, CDT has long argued that until we have an online privacy law that addresses all of the basic fair information practices, the privacy issues that we first saw 9 years ago in the collection of information via the web and then with cookies and then with spam and now with spyware and RFID and phishing will only repeat with new technologies in the future. A

privacy law that could get at a root concern rather than trying to define and scope each new technology in a limiting way.

This kind of privacy legislation would provide businesses with guidance about their responsibilities as they deploy new technologies and business models that involve the collection of information. At the same time, privacy assurances and law would give consumers a measure of confidence that their privacy is protected as companies roll out new ventures.

The legislation at hand today, H.R. 29, can serve as an important launching point that CDT generally supports. Representatives Bono and Towns deserve credit for raising the profile of this important issue in such a constructive manner. In particular, raising the penalties on bad practices can help the FTC create real deterrence.

On the other hand, CDT is less enthusiastic about the notice and other requirements on information collection programs in the current bill. We are concerned that the definitions are vague and may bring unintended consequences in the regulatory process that could serve to harm consumers. Instead, we would prefer to see this issue addressed in baseline privacy legislation so that consumers have a consistent framework for privacy and notice and consent across all technologies.

CDT is committed to working with the committee as your efforts continue, and I look forward to answering your questions.

[The prepared statement of Ari Schwartz follows:]

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

Chairman Barton and Ranking Member Dingell, thank you for holding this hearing on spyware, an issue of growing concern for consumers and businesses alike. CDT is honored to have the opportunity to participate in the Committee's first hearing of this new Congress.

CDT is a non-profit, public interest organization devoted to promoting privacy, civil liberties, and democratic values online. CDT has been widely recognized as a leader in the policy debate surrounding so-called "spyware" applications.[1] We have been engaged in the 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.

As an organization dedicated both to protecting consumer privacy and to preserving openness and innovation online, CDT has sought to promote responses to the spyware epidemic that provide meaningful protection for users while avoiding unintended consequences that could harm the open, decentralized Internet. Last year we testified before the Subcommittee on Commerce, Trade, and Consumer Protection on the issue of spyware, attempting to define the problem and suggest the range of responses required to address it. Since that time, we have worked closely

[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 650 responses). Center for Democracy & Technology, *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 (hereafter CDT Complaint Against MailWiper and Seismic). "Eye Spyware," 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 and Technology have leapt into the front ranks of the Net's spyware-fighters.")

with the Committee toward legislation to target spyware. We have appreciated the Committee's open, deliberative approach to this complex and important issue.

Summary

The alarming rate of growth of the spyware problem is a major threat to Internet users, as well as to the long-term health of the open and decentralized Internet. Of particular concern is the growing complexity of a marketplace that allows mainstream companies to unwittingly fund illegal activities through a maze of distributors and affiliates.

CDT sees three major areas where action is necessary to stem this disturbing trend toward a loss of control and transparency for Internet users: 1) enforcement of existing law; 2) better consumer education, industry self-regulation, and anti-spyware technologies; and 3) baseline Internet privacy legislation.

H.R. 29 marks a substantial step forward in addressing many of the concerns of consumer groups and companies. CDT is generally supportive of the current bill. In particular, we strongly endorse the idea of raising penalties on and calling specific attention to the worst types of deceptive software practices online. CDT is less enthusiastic about the specific notice and consent requirements on adware and information collection programs, because of the definitional difficulties in crafting such a regime narrowly targeted at certain classes of software. We look forward to continuing to work with the Committee to help improve these element of the bill.

On a broader note, we hope that work on the spyware issue will provide a jumping off point for efforts to craft baseline standards for online privacy, now that many companies have expressed their support for such a goal. Privacy legislation would provide businesses with guidance about their responsibilities as they deploy new technologies and business models that involve the collection of information. At the same time, privacy assurances in law would give consumers some measure of confidence that their privacy is protected as companies roll out new ventures.

If we do not begin to think about privacy issues more comprehensively, the same players will be back in front of this Committee in a matter of months to address the next threat to online privacy. We hope that we can address these issue up front, rather than waiting for each new privacy threat to present itself.

1. Understanding and Combating Spyware

What is "spyware?" No precise definition of spyware exists. The term has been applied to software ranging from "keystroke loggers" that capture every key typed on a particular computer; to advertising applications that track users' web browsing; to programs that hijack users' system settings. Much attention has been focused on the surveillance dimension of the spwyare issue, though it is in fact a much broader problem.

What the growing array of invasive programs known as "spyware" have in common is a lack of transparency and an absence of respect for users' ability to control over their own computers and Internet connections.

In this regard, these programs may be better thought of as trespassware.[2] Among the host of objectionable behaviors for which such nefarious applications can be responsible, are:

- "browser hijacking" and other covert manipulation of users' settings;
- surreptitious installation, including through security holes;
- actively avoiding uninstallation, automatic reinstallation, and otherwise frustrating users' attempts to remove the programs;
- substantially decreasing system performance and speed, in some cases sufficient to render systems unusable; and
- opening security backdoors on users' computers that could be used to compromise their computers or the wider network.

Each of these behaviors was specifically documented by CDT or reported to us by individual users frustrated by their inability to use their own systems. Although no single behavior of this kind defines "spyware," together they characterize the transparency and control problems common to such applications.

How can we respond to the problem? Combating spyware requires a multifaceted approach. Significant progress has already been made since the spyware issue first began to receive national attention over a year ago, but much ground still remains.

[2] Chairman Barton's statement at last year's Subcommittee hearing aptly expressed this idea: "[Spyware's] installation is often sneaky or deceptive and even when it runs, it often goes undetected . . . If I want someone to come into my home, I invite them into my home. If they come uninvited, it is a trespass." Doug Abrahms, "Anti-spyware bill drawing praise, support," *Gannett News Service,* Apr. 30, 2004.

- *Law enforcement*. Under federal law, much spyware is currently covered by Section 5 of the FTC Act, banning unfair and deceptive trade practices, as well as by the Computer Fraud and Abuse Act or the Electronic Communications Privacy Act. Spyware programs may also violate a variety of state statutes.
- *Private efforts,* including continued consumer education, the continued improvement of anti-spyware technologies, and stepped up efforts to close the security holes exploited by spyware purveyors, are all necessary. In particular, sound best practices for downloadable software are sorely needed.
- *Legislative* approaches to fighting spyware fall into two broad categories—attempts to narrowly address the issues raised by spyware, and attempts to deal, in a coherent and long-term fashion, with the underlying privacy issues. H.R. 29, which we address in detail below, is an example of the first approach. CDT has appreciated the opportunity to work with the Committee on this bill and is supportive of this effort. However, we remain firmly committed to idea that a long-term solution to spyware and other similar issues requires baseline online privacy legislation. Many of the issues raised by spyware may be easier to deal with in this context.

This framework represented our starting point on the spyware issue a year ago, and remains largely unchanged today. There have, however, been important developments in the problem, and in our research on the issue, since we appeared before the House Subcommittee last year. We address these in the following sections.

2. Spyware Continues to Grow as a Threat to Internet Users

When CDT first became involved in the spyware issue, we launched a "Campaign Against Spyware," calling on Internet users to send us their experiences with these invasive applications.[3] We indicated that we would investigate the complaints received and, where we believed appropriate, file complaints with the FTC. In our appearance before the Consumer Protection Subcommittee, we testified regarding the dramatic response to our campaign. In the nine months since our last appearance, CDT has continued to receive complaints through our online submission form. Among what are now hundreds of complaints, a total which continues to grow daily, are regular reports of new spyware programs arising.

While it is exceptionally difficult to obtain precise data on the prevalence of the spyware problem, the best study done to date, conducted by AOL and the Nation CyberSecurity Alliance, found that 80% of broadband and dial-up users had adware or spyware programs running on their computers.[4] Our perception based on the complaints we have received and our own research is that the prevalence of egregious spyware violations, including many mentioned in Section 2 of H.R. 29 before this Committee, has increased dramatically. Of particular concern is the use of security holes in web browsers to silently force software onto users computers. We believe many Internet users may simply be turning off the Internet in response to these threats.[5]

CDT was very pleased to see the first public enforcement action brought in October by the FTC against Samford Wallace and Seismic Entertainment on the basis of a complaint filed earlier by CDT.[6] This case included many of the clearly unfair and deceptive activities mentioned above, including browser hijacking and covert installation through security holes. We applaud the Commission for its work on the case, which has led to an injunction against further exploitative practices by Seismic.

The Commission's initial action against Seismic must be only the first step, however. First, many other parties were involved in the unfair and deceptive activities which CDT highlighted in our complaint to the FTC. We believe that the FTC's discovery in the Seismic case will provide ample basis to pursue these connections, and we expect that the Commission will announce further actions as other bad actors come to light. We discuss this affiliate issue in more detail below.

In addition, both the FTC and other national and state level law enforcement agencies must actively pursue further cases. While the FTC's first spyware case was an important milestone, both the number and frequency of cases must be dramatically increased if law enforcement is to provide a significant deterrent to purveyors

---

[3] *See* http://www.cdt.org/action/spyware

[4] http://www.staysafeonline.info/news/safety_study_v04.pdf

[5] *See, e.g.* Joseph Menn, "No More Internet for Them," *Los Angeles Times,* January 14, 2005, p. A1.

[6] There were instances of *private* enforcement against spyware purveyors that preceded the FTC's case. For example, in July of last year, 180solutions, a large adware vendor, sued a distributor that was using security holes to force 180solutions' software onto Internet user's computers in order to collect per-install commissions.

of spyware. Currently, we believe law enforcement is still losing the battle against egregious spyware purveyors clearly guilty of violating existing law.

3. The Affiliate Problem is at the Center of the Spyware Issue

In CDT's complaint to the FTC regarding Seismic Entertainment and Mail Wiper, we asked the FTC to specifically investigate the affiliate relationships between the parties involved. We highlighted the problem of affiliate relationship being "exploited by companies to deflect responsibility and avoid accountability."[7]

Since CDT testified before the Consumer Protection Subcommittee last year, it has become increasingly clear to us that the affiliate issue is at the heart of several aspects of the spyware problem. We want to take the opportunity in our testimony today to highlight and explain this issue, which has not been given sufficient attention to date.

Adware companies have a superficially simple business model: they provide a means of support for free software programs in a similar way that commercials support free television. Advertisers pay adware companies a fee to have their advertisements included in the adware program's rotation. The adware company then passes on a portion of that fee to distributors in exchange for bundling the adware program with other free software—such as gaming programs, screen savers, or peer-to-peer applications. Finally, the consumer downloads the bundle, agreeing to receive the advertising served by the adware program in exchange for the free software.

In fact, this simple description of how distribution of adware and other bundled software takes place is often a radical oversimplification. In fact, many adware companies and other software bundlers operate through much more complex networks of affiliate arrangements, which dilute accountability, make it difficult for consumers to understand what is going on, and frustrate law enforcement efforts.

The diagram below presents some of the actors and relationships in the online advertising world as we currently understand it. These include:

- *product and service vendors,* who have contracts with adware vendors and advertising brokers to distribute ads for their offerings;
- *adware companies,* who have multi-tier affiliate arrangements with other adware companies, software producers, website owners, and advertising brokers;
- *software makers and website owners,* who enter into bundling and distribution agreements with adware companies and advertising brokers, as well as with other software makers and website owners; and
- *advertising brokers,* who serve as middlemen in the full array of affiliate arrangements.

The consequence of these ubiquitous affiliate arrangements is that when an adware program ends up on a user's computer, it may be many steps removed from the maker of the software itself. The existence of this complex network of intermediaries exacerbates the spyware problem in several ways. For example:

- *Industry Responsibility*—Adware companies, advertising brokers, and others all may disclaim responsibility for attacks on users' computers, while encouraging these behaviors through their affiliate schemes and doing little to police the networks of affiliates acting on their behalf. Advertisers, too, should be pushed to take greater responsibility for the companies they advertise with.[8]
- *Enforcement*—Complex webs of affiliate relationships obstruct law enforcement efforts to track back parties responsible for attacks. The complexity of these cases puts an extreme strain on enforcement agencies, which struggle to tackle the problem with limited resources.
- *Consumer Notice*—Adware companies and their affiliates have been reluctant to clearly disclose their relationships in a way that is transparent to consumers. Appendix A excerpts a recent CDT submission to the FTC on this issue, demonstrating ways that adware companies could begin to improve transparency in bundling and ad-support arrangements. Companies have resisted these changes. Efforts to bring transparency to the full chain of affiliate and distribution arrangements have met with even greater opposition.

For these reasons, the affiliate issue has become a central aspect of the spyware epidemic. Finding ways to effectively reform affiliate relationships will remove a lynchpin of spyware purveyors' operations.

---

[7] CDT Complaint Against MailWiper and Seismic at 2.

[8] Examples of steps in this direction include public policies by Major League Baseball and Verizon setting standards for what software companies they will advertise with. Similarly, Google has drafted a specific public policy on what other applications it will bundle its utilities with.

4. Comments on H.R. 29, the "SPY ACT"

H.R. 29, before this Committee, represents the outcome of an extended drafting effort to target bad practices and bring responsibility back to the distribution of downloadable software.

The overwhelming support for this bill in the last Congress demonstrates the desire to craft targeted legislation focusing on some of the specific problems raised by spyware. CDT commends Representatives Bono and the Committee for your work raising the profile of this formerly silent plague on our computers. The focus of this Committee has allowed consumer groups and companies to bring the attention of the public and law enforcement agencies to this issue.

The current bill marks a substantial step forward in addressing many of the concerns of consumer groups and companies and CDT is generally supportive of the current bill. In particular, CDT believes that Section 2's focus on bad practices and its increase of the penalties for violators will serve as a valuable deterrent. H.R. 29 will give the Federal Trade Commission the clear authority and explicit mandate to pursue spyware purveyors. To this end, CDT also strongly supports the reporting requirement under Section 7.

CDT has been more hesitant to embrace Section 3 of this bill. The notice and other requirements on adware and information collection programs raise extremely difficult definitional issues which, if handled wrong, could have unintended consequences in the regulatory process that could ultimately harm consumers.

For this reason, the bill may be well served by another round of input from a wide range of parties in order to limit unintended consequences—especially in Section 3, where H.R. 29 deviates from the effort to focus on bad practices. CDT still believes that it would be most effective to address notice and consent issues in a general online privacy bill rather than a software specific bill, but we understand the desire to attempt to address this acute concern first, despite the complexities involved. We look forward to working with the Committee on this process.

CDT main concern is actually not with the bill itself, but the political process to move the bill forward. We do not want to see the passage of this bill be used to diminish efforts by this Committee or others in Congress to address online privacy in a long-term and coherent way. Rather we hope that the current effort on spyware can provide a jumping off point for efforts to craft baseline standards for online privacy now that many companies have expressed their support for such a goal. Otherwise, we will simply be back in this same place when we confront the next privacy-invasive technology.

We have very much appreciated the Committee's hard work and openness to comment in the anti-spyware legislation process, and we look forward to continuing to work with you on this and other digital privacy issues.

APPENDIX A

Adware companies face a particular hurdle in making their operations and value proposition transparent to users because adware programs typically do not run at the same time as the applications they support. In general, adware programs display advertisements while the user is surfing the web, regardless of whether the bundled game or file-sharing program is even running. This behavior can obscure the connection between the adware program and its bundled affiliate.

As one way to help address this issue, CDT has pushed adware companies—and the software companies they bundle with—to implement co-branding, putting the names and logos of supported applications on all advertisements. Although advertisements would still appear to users out-of-context, separated from the applications they support, co-branding would at least provide an immediately visible indication of the connection between the advertisements users see and the applications those ads support.

The mock-ups below show some ways that co-branding might be implemented. CDT submitted these same examples to the FTC's workshop on peer-to-peer file sharing applications. Some of these examples demonstrate more consumer-friendly labeling than others, but they all illustrate the fundamental principle of creating a visible link between adware and their co-bundled partners. Co-branding is needed because notice and consent at the time of installation is not enough. The ongoing operations of adware programs must also be made transparent.

To date, no adware company of which we are aware co-brands its advertisements.

Without Co-branding
(Adware Supporting a Single Application):

With Co-branding:

Without Co-branding
(Adware Supporting a Single Application):

With Co-branding:

Without Co-branding
(Adware Supporting Multiple Applications):

With Co-branding:

Mr. STEARNS. I thank the panel, and I will take the liberty, as Chairman, to start the questioning.

Mr. Schwartz, you have indicated sort of a little bit of concern here. What would you do today to improve the bill?

Mr. SCHWARTZ. Well, as I said, I mean, the main focus here on this bill—we generally support the bill, the—especially the focus on the bad—on bad——

Mr. STEARNS. So at this point, there is nothing you would change in the bill?

Mr. SCHWARTZ. Well, the concerns are about the definitions and more that a lot of it gets left to the FTC and the regulatory process, so it leaves a lot open for the FTC——

Mr. STEARNS. Yeah.

Mr. SCHWARTZ. [continuing] for FTC interpretation at this point.

Mr. STEARNS. Mr. Schwartz, anything in the bill—Mr. Schmidt, rather, anything in the bill that you would change today?

Mr. SCHMIDT. Well, generally, as—like Mr. Schwartz, I generally support it, and——

Mr. STEARNS. Support the bill?

Mr. SCHMIDT. [continuing] looking at some of the provisions that are in there, we have gone through four questions here in the past couple of days I would like some better clarity about on how those—the definitions are defined and who makes those decisions on those as well.

Mr. STEARNS. Mr. Rubinstein, what I am sensing is that everybody supports the bill, but they just want clarification of the language from our staff. Is that your feeling, too?

Mr. RUBINSTEIN. Yes, it is. There were a number of questions circulated by staff, and several of us testifying today are providing comments there.

Mr. STEARNS. Okay.

Mr. RUBINSTEIN. I think the cookie exception is an area worth exploring and should remain in the bill. I also alluded in my oral testimony to an issue around not allowing H.R. 29 to become a safe harbor for spyware vendors. And what I mean by that is, in the case of spam, for example, the fact that spam complies with the Act doesn't prevent ISPs from filtering spam or end users from deciding whether to accept mail or not. And similarly, in the case of spyware, even if a program does comply with this act, that shouldn't be viewed as a reason that consumers are obligated to download those programs. So in order for consumers to have full choice and for vendors to distribute very aggressive anti-spyware programs, we need to make clear that the bill itself does not change the legality in any way of programs that block spyware. So that shouldn't be pleated as a sort of defense by a spyware company. You know, I comply with the law, therefore the anti-spyware vendors should not be permitted to block my program. That should be up to the consumer.

Mr. STEARNS. I think that is a good point.

Mr. Baker, you were nodding your head. You agree with that then?

Mr. BAKER. I would generally agree with the comments by Mr. Rubinstein and the other witnesses.

Mr. STEARNS. Okay. And no one has any problem with the penalty side of this bill? I am assuming that that is acceptable, Mr. Schmidt?

Mr. SCHMIDT. Yes, I do. As a matter of fact, I think many of us have talked for a long time that we have got to raise the cost of doing bad things beyond the point where it is no longer——

Mr. STEARNS. That the bad actors feel it.

Mr. SCHMIDT. Yes, sir.

Mr. STEARNS. Yeah. Mr. Schmidt, I understand that you are a consultant to the Homeland Security. Is that true?

Mr. SCHMIDT. That is correct, yes.

Mr. STEARNS. Let me ask you, apart from this legislation, what steps should the industry and consumers take to enhance security on the Internet? If you had to protect a family member's computer for use on the Internet, what would you do and what functions would you allow to prevent others from spying on them?

Mr. SCHMIDT. You know, that is a good question. I think that breaks into two major categories. There is the maintenance piece of that, if you would, which is like an automobile. You need to keep oil, check your brakes, et cetera. And that goes to the security updates, the anti-virus software, the anti-spyware portion of the maintenance to the computer itself. The other is the educational and where they go. And I will use the analogy. One of my staff came up with this at one point. We could have the best shopping store in the country, but if you get mugged in the parking lot, you are not going to want to go there any more. So consequently, we have to do all we can, in addition to what enterprises are doing, to make sure that the consumers are aware of where to go, how to protect themselves, and Ralph there has good experience. And that is about doing trust and safety of the online experience as well.

Mr. STEARNS. Mr. Baker, this is a question. Does H.R. 29 adequately address the phishing problem? Does EarthLink, for example, educate its consumers about the phishing, both e-mail and web-based?

Mr. BAKER. Yes, Mr. Chairman, we do educate our consumers. We educate consumers generally about that and also—both let them know about the dangers of it and also provide tools to help. We have a program that uses heuristics to detect if they——

Mr. STEARNS. How would I——

Mr. BAKER. [continuing] if a website is phishy, if you will, and warn consumers away from that.

Mr. STEARNS. Now how would I, as a consumer using EarthLink, be told about this and use your program? I mean, do you proactively tell the consumer, or do you just tell them to go to your website or——

Mr. BAKER. Well, as part of the EarthLink software, we include the tools like Scam Blocker that blocks access to phisher sites and gives a notice to a consumer when they are—if they get a phisher—if they get an e-mail that leads to a website or if that looks like it is coming from a legitimate merchant, but it is actually a phisher site, the Scam Blocker program alerts the consumer to that. And we also provide information to our consumers as to ways you can also help protect yourself by looking, for instance, at the URL or

if you get an e-mail and you are not sure, rather than just clicking on the link that is provided in the e-mail, instead, go to your browser and type in the name of the merchant you are trying to get to. Whether that is EarthLink or eBay or Citicorp or whatever. So instead of just clicking on the link, which could take you to the phisher site, and again, they are made to look like the real thing, one way the consumer can protect themselves is, like I said, going and opening the browser and typing in www.Citicorp.com or www.Earthlink.net and that way the consumer can have some assurance that they are going to the correct website. So those are two of several different ways that consumers can protect themselves.

Mr. STEARNS. All right. My time has expired. The ranking member on our committee, Ms. Schakowsky, is recognized.

Ms. SCHAKOWSKY. Thank you, Mr. Chairman, and thank you for your testimony. I say that to all of our witnesses.

I wanted to—and we have talked a lot about what spyware can do to individual computers and to individual consumers, but one thing we really haven't talked about is the potential damages that a spyware infection can do to businesses, to Congressional offices. And I wondered if any of the panelists would like to fill us in a bit on those threats.

Mr. Schmidt, go ahead.

Mr. SCHMIDT. Yeah, I would be happy to. As a matter of fact, I alluded to that during my verbal testimony. What we have seen is sort of—as I have mentioned, sort of the additional pieces of spyware, which include Trojans, which then give someone an access to remotely control your system to create a bot network out of a robot network, which basically then could be used against critical infrastructure as a distributed denial service attack, keystroke capture to grab passwords, which generally not only relate to what you may be doing in your work environment, but also, oftentimes, your online banking and everything. So these things become very, very insidious as far as their ability to affect more than just an individual. And that is why corporations and enterprises are working very hard to make sure that they can wipe out the spyware on there, because it does affect their ability to manufacture, to provide—you know, for example, we have seen the situations in the past where airline reservation systems have been down for computer problems that could have conceivably been affected by spyware as well.

So it is your—you are quite correct. It is more than just about privacy and personal protection.

Ms. SCHAKOWSKY. That terrible situation we had during a snowstorm where all of the baggage was tied up, has that been attached at all to spyware, do you know?

Mr. SCHMIDT. Not to my knowledge, no.

Ms. SCHAKOWSKY. Okay. Mr. Rubinstein, according to a September 2004 article by Consumer Reports, Microsoft has found that spyware is directly responsible for more than 1/3 of application software crashes that might be linked to as many as half of the crashes Microsoft customers experience. Let me just ask you some basic—what does Microsoft mean by a "crash"? What does this do to a person's computer, to any files that they may have? And I am wondering if there is any way that you can estimate, in dollar

amounts, how much damage this has caused for consumers or for businesses or for Microsoft.

Mr. RUBINSTEIN. It is hard to put precise dollar amounts on the damage it has caused. I know that it is probably the leading reason for support calls, both to Microsoft and to the leading manufacturers, such as Dell, so that imposes, certainly, millions of dollars of cost on the providers of technology. In terms of crashes, spyware is often responsible for either slowing down the performance of a computer or simply not allowing the user to navigate to a selected site or even to use certain programs to stop pop-ups from interfering and so on. So it is certainly quite damaging, and I think the one point that I really want to call attention to is that the scenarios we have heard where I—the spyware tools are getting more sophisticated, but the scenarios we have heard where they were ineffective and where the consumer is forced to reformat a hard drive or replace a computer are just simply unacceptable, and I think that is why I think we need to bring together all of these different elements to combat the spyware.

Ms. SCHAKOWSKY. Finally, Mr. Schwartz has emphasized the need for baseline privacy legislation. I just wanted to ask the other three of you what your feeling was about the need to do just that. Mr. Baker?

Mr. BAKER. Privacy legislation?

Ms. SCHAKOWSKY. Baseline privacy legislation.

Mr. BAKER. Well, I think that—meaning this legislation, we have already taken a large step to protecting consumers' online privacy, because one of the insidious applications of spyware is, of course, transmitting personally identifiable information to another website without that user's knowledge. So this is—and so with or without stand-alone privacy legislation, this bill will—it takes a big step toward protecting consumers' online privacy.

Mr. RUBINSTEIN. Microsoft is committed to strong consumer protection of privacy, and we would be—we would welcome the opportunity to talk about legislation.

Mr. SCHMIDT. Yes, I think one of the things that I have always found very helpful is you look at legislation after market forces now, and I think with the collaborative effort that we have been looking at from the private sector agreeing on some baselines, if you would, for privacy protection, I think that would be the first avenue that I would recommend. And then if that, indeed, failed within a relatively short period of time, then I would look more toward the legislation. But even in that vein, I think the dialog that your leadership and Mr. Towns and Ms. Bono have done as well basically give us that vehicle that—to have the dialog to make sure we do things in the proper manner.

Mr. STEARNS. The gentlelady's time has expired. The full Chairman, Mr. Barton.

Chairman BARTON. Thank you, Mr. Stearns. We appreciate your leadership on this.

Let—Mr. Baker, your company purportedly has the best anti-spyware program on the market. Would you care to, in laymen's terms, explain to us why your program is reputed to be the best?

Mr. BAKER. Thank you. I suppose I should quit while I am ahead and not question the source of that assessment. But no, we do take

our customers' online experience very seriously, and so we have developed, either on our own or in conjunction with other companies, various applications, like Spy Audit that, again, lets a user—it lets anybody, you don't even have to be an EarthLink customer, scan their computer to see what spyware is on there. And then if you are an EarthLink customer, you have a spyware blocker that lets you disable it. And it is—we are just always working. It is almost like an arms race. You know. We devise tools to block spyware and to remove it and at the same time, the folks who write this nowware, as it is sometimes called, spyware and other bad applications are always, you know, trying to find ways around the protection. So it is just a question of constant innovation and getting feedback from customers and finding out where this is coming from and designing tools and systems to help consumers enhance their online experience.

Chairman BARTON. Why do you think the perpetrators of spyware—what is the potential gain that causes them to try so hard to get around the anti-spyware programs and to invade people's computers? What is it that they gain by successfully putting spyware on an individual or corporate computer?

Mr. BAKER. Well, that depends on the form of spyware. In the case of the less intrusive and less insidious adware, it is just a question of revenue. One site pays—one website will pay another website when a cookie or another piece of adware indicates that a customer got to website B, having first visited website A. So there is—money changes hands there. In the case of phisher sites that Mr. Stearns mentioned earlier, while those are not strictly spyware, clearly the motivation there is that if the perpetrator can steal a consumer's credit card number or bank information or other information, then obviously there is—money can be gained there. In the case of other forms of spyware, it is just malicious. It is online vandalism. And I guess——

Chairman BARTON. So there is no financial——

Mr. BAKER. [continuing] in some cases, there is no direct monetary benefit, other than just the malicious harm that can be done to an online user, their Internet provider, their software provider, their——

Chairman BARTON. Well, this is a question for all of the panel. Who are the generally guilty parties in the spyware business? Are they businesses seeking financial gain, or are they college students and teenagers just trying to do it for the heck of it? Who are we—who is the enemy?

Mr. SCHWARTZ. There are a lot more businesses out for financial gain at this point than there have been in the past. As we map it out in our testimony, this chain of affiliates and distributors that has been created through the process of which distributor—software gets distributed online, and it has created this kind of incentive for making the ends justify the means of getting this software on people's computers. So an advertiser might not know how this software got on someone's computer, and the person who is actually delivering the software may not even know. There are—all of these affiliates in the middle, six or seven layers worth of affiliates who are all getting paid up and down the chain. And so therefore, someone in the middle is completely unscrupulous and has no—doesn't

really care how the consumer gets it. The people at the top and the bottom may care, however, the website that is actually interacting with the consumer may care. The company that is advertising may care. But the people creating the software and creating the means to try to get it on the computer often do not care. And they are making a good deal of money out of getting this software onto people's computers.

Chairman BARTON. So in general, you all agree it is business. It is that people are in it for some sort of propriety gain that are the perpetrators. We have some of them that do it just for the heck of it, but most of it is really a business for business reasons. Would you all agree with that?

Mr. RUBINSTEIN. I think that is right, Mr. Chairman. There is a sense in which spyware is beginning to replace spam as a—kind of an opportunity for unscrupulous business people. But I think there is also a growing trend for more serious organized crime, taking advantage of spyware to create, as Mr. Schmidt indicated, these so-called bot nets or zombie networks that allow them to take control over a machine, and then sometimes, you know, have a group of thousands of machines, which they rent or sell to these businesses to further spam schemes or phishing schemes. So we are seeing more of that as well.

Chairman BARTON. Well, my time has expired, but I want to thank all of you gentlemen for your testimony today. I thank the full committee chairman.

The gentleman from New York, Mr. Towns.

Mr. TOWNS. Thank you very much, Mr. Chairman.

I would like to ask you, Mr. Baker, when a consumer's computer crashes, he often calls the software or the hardware provider for assistance. This technical assistance costs companies in the millions. What types of costs are incurred by Internet service providers, such as your company, as a result of the spyware? In other words, let me put it this way. How much is spyware costing your company?

Mr. BAKER. Congressman Towns, I don't have an exact figure on it, but it is literally in the millions and millions of dollars, because, as you have pointed out, customers can call into their ISP, and you know—an Internet provider kind of exists at a crossroads between hardware and software, between the user's individual computer and the Internet at large, and so any time something affects any of those systems, the consumer is going to look to their Internet provider as to why they can't get online. And so it generates a call to our call center and—or sometimes e-mail or sometimes chat, but it drives up the contact rates, it drives up the times that our reps are on the phone with customers, and you know, sometimes it is easily resolved and sometimes it is not. Obviously that causes frustration to the user, and it does increase our costs, so again, I don't have an exact figure on it. I would be happy to provide that to you and get you an estimate, but again, it is in the millions of dollars per year.

Mr. TOWNS. I would appreciate it if you would.

To you, Mr. Rubinstein, first let me thank you, Microsoft, for their support of this legislation. We appreciate that. And I was pleased that your written testimony noted that we had successfully

focused on bad practices. Throughout this process, it was critical to me that we craft legislation that does not hamper legitimate software applications and activities, like computer security, diagnostic, and technical support. You talked about shared responsibility for tackling spyware, taking into account the legislation and the progress in the different areas identified in your testimony, how close are we to solving the spyware problem, and what more should industry be doing?

Mr. RUBINSTEIN. Thank you, Congressman Towns.

I think there has been substantial progress on consumer education, making that available. There are a number of excellent sites, and I can provide those, if you like. I think the anti-spyware tools are becoming more sophisticated as well. I think the two areas where there really needs to be more attention and focus are first around industry agreeing upon best practices for good software. It is very useful, as we have found in the spam—in the anti-spam effort to have both safe lists and block lists. So if you can have criteria that legitimate software follows for installing itself, for example, and then have a way of representing that a given program is actually safe to install, that aides the anti-spyware tools in really focusing on the bad actors and being more effective. So I think that is something that industry needs to move ahead on. There have been several best practice guidelines distributed both Center for Democracy and Technology and the Online Privacy Alliance have been active in that, but I think more needs to be done.

I also think that a key technological development is having not only a detection and removal capability in the spyware tools but also real time protection, which means that as the spyware attempts to load itself, the tool is actively blocking it in real time, so that you don't have to get hit and then try to recover. You are actually protected as you surf the web.

And finally, I think, from a technology standpoint, the important future development will be protection at the enterprise level, by which I mean not just at the level of an end user's machine, but the ISPs, the large enterprises, like the House or the Senate or universities blocking spyware before it even enters their systems so that it is not up to the end user to do that, but it is instead taken care of at a more systemic level.

Mr. TOWNS. All right. Thank you very much.

Mr. Chairman, very quickly. Mr. Schwartz, many consumers continue to download software infected with spyware so they can illegally trade music or movies. Do you think that most consumers know that they are putting at risk the operation of computers, which may cost $2,000, $3,000, or $4,000? What more can we do to educate the public about the dangers of spyware?

Mr. SCHWARTZ. In our testimony, we document some examples of how we could highlight better how people actually got the software down on their—down to their computer, that forcing some of the advertisers to start engaging in the best practice discussion, as Mr. Rubinstein said earlier, that we are starting to move toward a more—a better discussion of best practices for advertising I think will illuminate a lot of the issues in terms of peer-to-peer in particular. Representative Murphy raised the example of Gator or Gain, and that is exactly what we are—we mock up on the back

of—Kazaa, which is a peer-to-peer program, now comes with Gain when you—when a consumer downloads it, they get Gain, which acts—which runs, actually, while the person is on the web, not while they are using the other program. So they might even know that it is advertising supported, but they wouldn't necessarily know what program it is or how it works. It is very confusing to consumers. So we are trying—we suggest trying—moving toward best practices of making them co-brand, so that when you go to remove the software, you know that it came because you had Kazaa. When you get the ad itself, you start seeing these pop-ups, you know that it came because you have this peer-to-peer software on your computer.

Also, it shows—it should show up on the add/remove file. As you know, it does not, today, show—the products in Gain does not show up in the add/remove file. It makes it very difficult for consumers to be able to remove it. These are just common best practices that software should have to file, and that is exactly along the lines that we think—where we think we should be moving, as Mr. Rubinstein referred to earlier, toward best practices.

Chairman BARTON. I thank you, Mr. Schwartz. The gentleman from Georgia, Mr. Deal.

Mr. DEAL. Thank you, Mr. Chairman. And first of all, I would like to welcome my friend, Mr. Baker, to the panel today and for those of you who don't know, he was formally an elected public service commissioner of our State survey, I believe, in his former life, and we are pleased that he is here taking a position on a cutting-edge issue that affects all of us.

I have been looking at the enforcement provisions of this bill, and I would like to ask you a couple of questions, anyone on the panel, quite frankly, as to whether or not the enforcement provisions we provide are adequate or whether or not we have the potential of doing some harm here. And let me highlight a few of the issues that I am concerned about. As I read the bill, the primary—the exclusive enforcement provision is through the FTC. And it only outlines civil penalties, financial or civil penalties. Are there potential criminal penalties associated with this activity under the referenced sections to the existing Federal Trade Communication Act? I don't think so since it goes ahead here and it says the exclusiveness of the remedies are those outlined here in this bill. So are we only talking about civil penalties, as you understand the proposed Act? Anybody?

Mr. RUBINSTEIN. Yes, Congressman, I believe that is correct. I would point out, though, that there may be criminal complaints that could be brought under the Computer Fraud and Abuse Act for at least some of the more egregious bad practices that would be viewed as computer abuses under that statute.

Mr. DEAL. Okay. I am concerned that we talk very much here about exclusiveness of remedies and we hinge it all to conduct defined in this Act and make it the exclusive remedy. Let me tell you another concern that I have, too, and that is the preemption clause of the statute. As Mr. Baker knows, our Governor has recently announced an aggressive State proposal to deal with spam through State statute. I believe he is proposing to make it a felony. He is mad about it, as you can tell. We are here preempting State laws.

It is a little bit strangely worded to me, however. It talks about preemption of State law, and it says anything that is the prohibited conduct described in sections two and three. And then it goes, on the next page, to talk about that only an attorney general of the State may bring a civil action under the law of any State if such action is premised in whole or in part upon the defendant violating any provision of this Act. Does that take local district attorneys at the State level out of the picture of enforcing anything that would relate to this? And if so, what is the venue? That really, to me, is a primary concern. If it is a criminal act, the venue is where the act is committed, not where the defendant is located, which is the venue for civil penalties. Would somebody expound on that area?

Mr. BAKER. If I may, Congressman, and thank you for your kind words.

As to venue, I believe we have a situation where as long as any part of that transaction touches where the consumer is, the violator may or may not be in that same jurisdiction, but if the harm—where the harm is done is sufficient for venue.

And to your earlier question as far as the exclusive remedy and enforcement and preemption issues, I would look, by analogy, to exactly the situation that you mentioned with spam where we had Federal legislation in the form of the Can Spam Act. And there were some preemption sections in that. However, that did not totally preempt State laws, either those that were already extent or, as in the case of Georgia, ones that are being introduced, so it is possible to still have Federal legislation without completely preempting—Federal legislation with a preemption clause, it still does not completely preempt State laws, which would complement it. And again, to give you an example of our own efforts in fighting spammers. Even before the introduction and passage of the Can Spam Act, EarthLink still sued spammers. We probably sued about 100 to date and have various counts in those complaints, whether that is Federal laws, like Computer Fraud and Abuse Act, or State laws, whether they are rather more recent laws that are specifically technology related or whether they are just long-standing common law notions of nuisance and trespass. So we have always had the ability and maintain the ability, whether it is a spammer or a purveyor of spyware, to go after them. But—so we view Federal legislation like this as a complement to those efforts and notwithstanding preemption clauses that may be in it or specific requirements for exclusivity of enforcement as pertains to that law. There are still other counts that an online provider could use in going after these folks or State attorney general or another entity. So——

Mr. STEARNS [pesiding]. The gentleman's time has expired.

Just a point of information, some of the most egregious acts, spyware acts, I think are covered under the Wire Fraud Act. So we already have existing statutes to cover that, and obviously with the bill we have, since our jurisdiction is the Federal Trade Commission, you know, we would not have an criminal penalties in it.

The gentleman from Washington, Mr. Inslee.

Mr. INSLEE. Thank you.

Ira, I wanted to thank you for Microsoft's effort, but this is a little off subject. I would also like to thank a fellow who works for

Microsoft who made a contribution of $750 million to the International Vaccine Effort yesterday. We appreciate that effort, the whole Microsoft family.

But I want to ask you about your Microsoft protection efforts. Could you just elaborate on what your experience has been on the new product that you have made available in a sense? You refer to it generally. How many people have accessed it? Has it worked? Have you had any difficulties? Are there ways around it? How are you doing with the international folks? Just if you can elaborate on it.

Mr. RUBINSTEIN. Thank you, Congressman Inslee.

We acquired a company called Giant in late December, and we committed to release it as a—release their anti-spyware tool as a Microsoft product within a month, and we are very happy that we met that goal. And the figures I have are that in the last—in the first 2 weeks of January, at least, there have been more than 3 million downloads of the tool, so we are very pleased to see that positive feedback. We think that the tool has a number of interesting features beyond just detect and removal. As I pointed out before, it also has a real-time protection aspect to block spyware as it is downloaded. And it also creates, on an opt-in basis, something we call spynet, which allows consumers to report suspected spyware and then have that investigated on a priority basis and quickly added to the list of spyware programs that the tool detects. So we have taken the power of the Internet and turned it, you know, toward identifying more spyware and doing so very quickly.

Our plans are to accept consumer feedback for several months to begin working on localization of the product and then to release it as a full-fledged product some time probably in the first half of this year.

Mr. INSLEE. Got you.

A question for the whole panel. Talk to us about our international efforts from offshore folks. What is our best protection against that? What strategies should we be thinking about that are not in this bill? What are you doing about it? We are looking for brainstorming here.

Mr. SCHMIDT. Thank you, Mr. Inslee, and it is good to see you again, sir.

It is interesting, because that is very closely aligned to Mr. Deal's question relative to the States where you have, you know—what is not in anybody's best interest is 50 different statutes or 50 different sets of regulations relative to this. You compound that tremendously by going international. So currently under the G8 Subcommittee on Cybercrime, which the State Department and the Department of Justice have been gracious enough to invite many of us from private sector to participate in that, we are working on the international realm as well, trying to use that same framework that has been established in this bill to try and internationalize that. It is very, very challenging, because some people view this truly as criminal. Some of the countries we deal with don't even have any laws close to the cybercrime piece of it, let alone the civil penalties, the provisions that this Act provides. So we are working that.

Also, in a private sector perspective, Microsoft, Yahoo, eBay, and AOL recently met in Asia with a number of the countries in Asia and signed a Memorandum of Understanding on working collectively on a proactive basis, as Mr. Rubinstein pointed out, to prevent these sort of things from happening.

So there are a lot of efforts, but none of them have been put together in a fashion by week and say in 6 months, we are going to have a solution. But it is not being ignored, by any stretch of the imagination.

Mr. INSLEE. So if you look forward to the passage of this bill, does it just drive these folks from one country to another as we increase our international agreement, which I presume will start with G8, but I don't know how many countries there are, but there are a lot more than eight, is this—are they going to be one hopscotch ahead of us constantly until the world is under this bill we are going to pass or what do you think?

Mr. SCHMIDT. Yeah, it is interesting. Mr. Deal was asking a question while I wrote a note to myself, and relating back to the old issue, we dealt with telemarketers. And actually, we were forming, sort of, safe harbors for them, because they were hiding under certain States under the provisions where they felt they could operate in exemption. And that is correct. And we are, indeed, worried about that aspect of it.

And relative to the G8, by the way, even though it is the G8 Subcommittee, we have over 110 nations now that are a part—participating in that proactively as well as some multilaterals as well.

Mr. SCHWARTZ. But one point to add on to that is that the Federal Trade Commission has really been moving, and they really recognize exactly this problem that you raise, that as we move into more of a network world, we are going to see—start seeing the bad guys move offshore and move their businesses offshore and have—has started to try and build alliances and started—start to work on some of these issues. This committee dealt with it—this issue in the crossborder fraud legislation that came forward, that the FTC has been pushing forward. And there have been other efforts that the FTC has been working on. So I think this is a question that goes beyond just spyware. It is really a question of how are we going to do enforcement for the Internet generally. One thing to point out, though, is it is going to be very expensive to do the kind of forensic works you need—work you need to be able to track people across the world—around the world. Just giving more power to the FTC is not, alone, going to do it.

Mr. INSLEE. Ira, I think you made reference to you don't want to create a safe harbor that doesn't exist now. We always want to retain consumer choice here. Have we solved that problem or is there specific language you would suggest or——

Mr. RUBINSTEIN. There is language in the Can Spam Act that goes in this direction. There is also a Good Samaritan provision in this Act that might be adjusted to deal with the issue that I identified.

Mr. INSLEE. Should we use the Can Spam language in this bill?

Mr. RUBINSTEIN. I think that would be appropriate. We have just begun to discuss that with staff, so we are in the early stages of addressing it.

Mr. INSLEE. Thank you. Thanks, folks.

Mr. STEARNS. I thank the gentleman.

The gentleman from Arizona, Mr. Shadegg.

Mr. SHADEGG. Thank you, Mr. Chairman. I want to thank the full committee chairman for this hearing. I want to thank you for your interest in the topic, and I want to thank our witnesses. When this legislation appeared before this committee before, I made it clear that I view it as of deep concern. There are many different versions of spyware and probably far too many for me to begin to comprehend, maybe even too many for any of you to comprehend in terms of what all is out there. But I have at least one basic understanding of spyware, and that is keystroke recording, which takes me back all of the way to the days when we had wire tapping. I think the American people are deeply concerned about their privacy interests, and I think that if they understood that someone was wire tapping their phone, either at home or at work, they would be deeply upset. And I am not certain that when the average American hears the word "spyware" that they have an understanding that this is the electronic, or at least one aspect of spyware, is the electronic equivalent of wire tapping, where they record every stroke I hit on my computer. I want to—I think it is extremely important that we get beyond the internal Congressional disputes on this legislation and that we, in fact, pass something and that we pressure our friends in the Senate to pass something on this topic. I think it would be a serious failure if we don't do that. I recognize that the industry has reservations about what precisely should be done, and I am more than willing to listen carefully to those reservations and try to craft the language as carefully as we can. If, as was just suggested, there are other definitions that should be lifted from other draft legislation and placed in this bill, I would support that, but I think it will be inexcusable if this Congress fails to act in this area.

I share Mr. Deal's concern about the issue of preemption. It seems to me if the American people understood that this is the equivalent of wire tapping and then understood that we were preempting a State's attorney general's office from going after the equivalent of wire tapping where someone was, essentially, gaining access to their personal computer and then recording everything they do on that computer, no matter what expectation of privacy they had, they would not be happy about that. The chairman of the committee indicated that there are other penalties. I guess I would like to ask you, Mr. Chairman, or counsel, if those penalties include criminal penalties that would go at keystroke recording so that we can get at—so that we are assured that there is, in fact, a criminal penalty for somebody who essentially wire taps through this mechanism.

Mr. STEARNS. The gentleman—I understand from staff it is currently a felony.

Mr. SHADEGG. Okay. Is that—if I might as the panel—the chairman—the members of the committee—or the panel, is that your understanding as well?

Mr. SCHWARTZ. Yes.

Mr. SCHMIDT. That is correct, sir. Yes.

Mr. SHADEGG. And are those penalties currently being pursued by either U.S. law enforcement officials, U.S. attorneys and others across the country, or are there similar penalties at the State level?

Mr. SCHMIDT. If I may speak from the perspective of a State local law enforcement from my days at Chandler Police Department, and of course Arizona was one of the early States that passed criminal statutes relative to a vast array of computer crimes. I called my son when I was preparing for the testimony. I said, "Well, how many cases do you actually get at Tempe on people complaining about spyware?" And he says he gets very few, because they don't understand.

Mr. SHADEGG. Right. They don't even know it is happening.

Mr. SCHMIDT. That is correct. They call and they ask how to remove it, but not the provisions of how to prosecute someone. And I asked him, "Well, if you were asked to do that, how—would you be able to do so?" And he said, "Right now, there is just—the resource is not available for State and local law enforcement to be able to successfully do those in any numbers at all."

Mr. SHADEGG. I think it is important that we do that, because, as you know, a good part of criminal law enforcement is prophylactic. That is to say, you enforce the crime against somebody and you make an example out of them, and that discourages anybody else from engaging in that conduct. And so it seems to me that it is important that we act in that regard. And——

Mr. SCHMIDT. One quick comment, if I may, Congressman. It may be just a little side note to this. And I have been encouraging a number of law enforcement folks I have dealt with across the country, as part of their crime prevention efforts they do is they send out brochures on how to put burglar bars to protect yourself. Do something very similar to these sort of acts to help do the very preventative nature of it so we can reduce the number of activities that take place that need to be investigated and prosecuted.

Mr. SHADEGG. Now I think that is important and I think that far too many Americans are unaware of the fact that spyware can be essentially very criminal conduct that can invade their privacy in very specific ways and can be very serious, and in the business world, could, in fact, be financially ruinous.

So I appreciate your testimony here today. I appreciate your support of this legislation. I look forward to working with you to ensure its passage. It seems to me we have failed last year. We dare not fail this year.

With that, Mr. Chairman, I yield back.

Mr. STEARNS. I thank the gentleman for his good comments.

The gentlelady from Wisconsin, Ms. Baldwin.

Ms. BALDWIN. Thank you, Mr. Chairman.

Mr. STEARNS. And I would just also welcome you to the committee, and we are delighted to have you.

Ms. BALDWIN. Well, it has been a delight, actually, to have this as our first hearing of the session, and I will take advantage of being a newcomer and ask some questions that perhaps I wouldn't get away with as a senior member of the committee.

In this discussion, we do not have a representative of the Federal Trade Commission testifying today, and there has been some discussion, I think, Mr. Schwartz, in your testimony, you were talking

about the fact that we have to dramatically increase investigations enforcement if law enforcement is going to serve as a deterrent. You discussed, also, in your testimony, the specific case that you brought before the FTC and pleasure that it was taken seriously and investigated and will lead to others. But the legislation before us will give the FTC more specific power. I would like to hear about the resources that go along with that. Are you seeing an increase in the investigations, the enforcement efforts that are going on at the FTC?

Also, let me throw a second question out, and any of the panelists who feel comfortable answering it, can. We are talking about the State level. Have you seen promising investigations of enforcement at the State level at this point that can add to the dramatic increase that is going to be necessary for a sufficient deterrent?

Mr. SCHWARTZ. To follow-up on the FTC question, we—they don't tell us about ongoing investigations. They—it is against their rules to do that. So we don't know how many they have. They have told us that they are investigating cases, and certainly, when we have gone to brief them on certain things that we have been seeing, there have been more people in the room now than there were a year ago. So that—it seems as though that is a positive sign toward doing more—toward doing better enforcement.

The issue, I think, of the complexity, though, of these kinds of cases really does go to your point in terms of needing more resources to be able to do something like this. Taking this on on our own, and when we did the Seismic case, it took us a great deal of time just to map out the different players and the—that were involved, and still of them we still don't know, to this day. It takes the FTC the ability to do the same kind of mapping and then go in and get discovery and find out all of the players involved and then go through all of their files and find out all of those players involved. It is quite an extensive process to do one of these—the forensics for one of these cases together. And I don't want that to be lost, because certainly raising the penalties does give them more power, but it doesn't serve as a deterrent if you can't use it.

Mr. SCHMIDT. I would like to make two quick comments on that. For the FTC, particularly Commissioner Swindle has been a leader in this area, from FTC working, not only with the Congress as well as private sector, but also the OECD. But it is tantamount to drinking from a fire hose is what it boils down to, which is why a lot of the efforts we are doing, and we are hoping this bill helps, is become an incentive not to do these sort of behaviors so we can get it down to something that is manageable.

The other thing relative to FTC, like any other law enforcement agency or any investigator or regulatory body, they just don't—will never have the resources, which is why they are oftentimes augmented by their counterparts in private sector. You know, the provisions of Title 182703, which gives us the ability to protect our networks, we can collect a lot of information and turn that over to FTC or turn it over to law enforcement, which they may have the challenges in doing so with the lack of resources. So we can actually become very good partners, and we have seen that happen on a regular basis.

Mr. RUBINSTEIN. I would just add, Congresswoman, that Microsoft, EarthLink, AOL all now have a long history of bringing hundreds of lawsuits in the spam arena, and I think we are all starting to gear up additional legal and investigatory resources to devote to some of these new threats, such as spyware and phishing. So we hope to bring more cases and to cooperate both at the Federal and the State level.

Ms. BALDWIN. Any comment about the State level enforcements or investigations that have been helpful in this?

Mr. SCHWARTZ. Well, there haven't really been that many State level enforcements. We have been contacted by a few attorney generals and a few State district attorneys as well on certain cases, but again, it is—cases are extremely complex, and we haven't been able to really map out those cases in the same way that we could in the Seismic case. I know that they have resources that they are putting toward it, but we haven't seen the fruits of the labor yet.

Mr. STEARNS. You are all finished? Complete. Okay.

The gentleman from Pennsylvania.

Mr. MURPHY. Thank you, Mr. Chairman.

I have a few questions I just want to ask in general and see if—who can answer these, but they are—some of the specifics have been raised today about the bill.

Mr. STEARNS. Okay.

Mr. MURPHY. For example, does this bill adequately require every download of information at the computer software to be an opt-in? Does it adequately—is the wording adequate for that? I will go a few more, and if you can't get it for me today, maybe you can get it to me eventually, or get it to the chairman.

Does it—Mr. Schwartz, you mentioned the add/remove file. Does the wording in the bill adequately address that anything that is downloaded has to be visible and it can't be hidden for an add/remove file, and further that it be visible in search files or in program files when one gets into those areas? Do you know if the wording in the bill adequately addresses that?

Mr. SCHWARTZ. Well, this is some of the difficulty of doing this on a technology-specific basis. It is hard to know. I mean, this is exactly the—was my point earlier about the definitional issues. It is hard to know exactly how this is going to lay out, how the definition of software information collection programs are going to work themselves out in the regulatory process. So it is hard to know today to be able to say yes it adequately covers it or not. We would prefer to have—to cover this across technologies and say it is the collection of information, it is—and it is the transparency issue, as you have raised, that are important that consumers understand that their information is being used in that way, at least for the privacy aspects of this.

Mr. MURPHY. Well, that—and Mr. Chairman, maybe I can just state this in general and hopefully have these sent back to the committee from our experts. But other areas, too, and that is does it prevent some software from lying dormant and then sometimes reemerging to do this so that if one is even searching for files to find if anything has been downloaded that it really is visible at the time of downloads? Does it also prevent these things from attaching itself to e-mails, because that is oftentimes how things come on

computers surreptitiously or cloaking itself as a legitimate website, as was brought up, too, and then a person thinks they are going to a legitimate link and then it turns out to not be or—and I guess all of these mechanisms, and more that we can't even anticipate yet, because as soon as you make something illegal, someone else will come up with a technique to make—to find another loophole there. But that is why—although we are looking for specifics to still come up with enough general ideas to prevent some of these from surreptitiously or illegally or at least without informed consent to have some of these, and I am hoping these are—this is information that the committee can, perhaps, get back to us in writing, back to the chairman. I would love to have that review.

Thank you, Mr. Chairman. No further questions.

Mr. STEARNS. Well, thank you. I think what we can do, Mr. Strickland, you are next, and I think we have got a vote, but I think we have got sufficient time for you and then——

Mr. STRICKLAND. One question and then a quick question.

Mr. STEARNS. Okay.

Mr. STRICKLAND. And I am sorry I wasn't here, but I had a meeting earlier for the testimony.

Mr. STEARNS. I understand. We all understand.

Mr. STRICKLAND. But I just wanted to ask you, do you think that this bill, as written, will deter innovation in e-commerce?

Mr. BAKER. No, I——

Mr. STRICKLAND. Anyone can answer that. Yes, no, or if you want to elaborate.

Mr. BAKER. Let me—that is clearly not the intent of the bill, and I don't think it will. What we need to do with this bill, or any legislation, is go after the bad actors, and I think this bill does a good job of doing that. I mean, clearly, it is not meant to apply to the operating system, the Microsoft operating system that comes preloaded on the computer or the EarthLink software that allows an online user to connect to the Internet.

Mr. STRICKLAND. I understand. And you know, sometimes we pass well-intentioned legislation, and then we find out later it has adverse consequences, and I was just—you know, thank you for your opinion. I don't challenge your conclusion. I just wanted to ask the question to see what it was that you thought in terms of this particular matter. So thank you, sir. Thank you.

Mr. RUBINSTEIN. If I may supplement that answer, Congressman. I think the section two, which focuses on bad practices, will not have that impact. But section three, where there is some very crucial definitions that try to balance the types of scenarios where information needs to be exchanged in the background, because it is just the way the Internet works, those are very important provisions. In particular, we don't want, in the name of going after spyware actors, to have a transformation of the user experience so that when you go to a website you just get bombarded with consent dialogs: "Is it okay to do this?" "Is it okay to do this?" "Is it okay to do this?" And as long as we maintain that balance between requiring notice and consent in certain cases but accepting it in sort of the ordinary use of cookies, just for shopping carts, for identifying customers, et cetera, then I don't think it will have any adverse consequences.

Mr. SCHMIDT. In short, Congressman, it is unlikely that it is going to have a bad effect, but we want to make sure, and to Mr. Murphy's question about the definitions of some of these things, a lot of the things we are working on, for example, I am not here on behalf of eBay, but I know eBay is—we have launched an account guard, which automatically does sort of the delineation between good sites and bad sites to protect consumers very proactively that requires that download and in the early version of this, it would have inhibited our ability to do something like that. So we want to make sure that we continue to make sure there is a clear demarcation between the bad actions and the things that are a benefit to the consumers. Thank you.

Mr. SCHWARTZ. I basically agree with everything that has been said here, but I would also like to point back to Mr. Rubinstein's comments earlier that were not part of my testimony, but I agree with the idea that we need to be careful about the anti-spyware tools and making sure that we are not limiting the ability for anti-spyware tools to gain the consent of consumers to be able to do this so that they can continue to innovate, too. That is an extremely important key to make—to this effort to stop spyware is going to be the technologies.

Mr. STRICKLAND. Thank you, Mr. Chairman.

Chairman BARTON. Thank you, Mr. Strickland.

We have a series of votes on. There are no other members present, and I am told on the Minority side that there are no members wishing to come back and ask questions, so I am going to conclude the hearing. I want to thank you gentlemen. I will make an announcement before we formally adjourn. We are going to take the comments on the bill, as introduced. The deadline is, I think, close of business today. It is not a mistake that the—in the last Congress this bill was H.R. 2929 and in this Congress it is H.R. 29. I think that shows you how the priority has shifted. We expect to be ready to move this bill very quickly, probably, within the next 2 to 3 weeks. If the comments come in as favorable as our verbal comments have been, we are aware of a few minor issues that we agree need to be clarified, but because of jurisdictional reasons, I don't think we are going to do that at the committee. We will probably do that on the floor or in conference when we go to conference with the Senate.

So this is on the fast track, and we will hope to be marking this bill up in the very near future. And gentlemen, I wish to thank you and all of you—the interest groups that you represent for your attendance and your support for this bill.

This hearing is adjourned.

[Whereupon, at 12:07 p.m., the committee was adjourned.]

[Additional material submitted for the record follows:]

PREPARED STATEMENT OF WEBROOT SOFTWARE, INC.

EXPERTS AT COMBATING SPYWARE

Webroot Software, Inc. appreciates the opportunity to provide written comments in conjunction with the Committee's hearing on H.R. 29, the Spy Act.

Webroot, a privately held company based in Boulder, Colorado, was founded in 1997 to provide computer users with privacy, protection and peace of mind. Today, Webroot provides innovative products 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.

Webroot, maker of the award-winning Spy Sweeper, is the industry leader at combating spyware. Earlier this month, Webroot introduced the anti-spyware industry's first automated spyware research system. The new system, called Phileas, uses "bots" to continuously comb the Web, uncovering spyware, adware and other types of potentially unwanted software that are deeply embedded on web sites. One hour of automated research is the equivalent of approximately 80 hours of manual research. The bots visit millions of sites per day, identifying and archiving the HTML sources and URLs in Webroot's spyware definition database—the largest and most accurate catalog of spyware definitions. New definition updates are then developed by the Webroot Threat Research Team and distributed to Webroot customers, before their systems are infected by these programs.

In the first production use of the system, it identified more than 20,000 sites used to deploy spyware through drive-by downloads, as well as several new spyware variants. By February 2005, Webroot will deploy more than 100 bots online to track all forms of spyware and adware, with each bot visiting as many as 10 URLs per second, collectively visiting over 80 million URLs per day.

THE PROBLEM GROWS LARGER EVERYDAY

These technological advances are vital to combating spyware, as the problem grows larger everyday. Since the committee first began work on spyware legislation in Spring 2004, the incidents of spyware have mushroomed.

Seven years ago, Webroot's detection list included about 200 pieces of spyware. By March 2003, the detection database included 700 pieces of spyware. Today, Webroot's database lists over 2,000 pieces of spyware, reflected in over 50,000 traces, and this number continues to rise rapidly. Most weeks, Webroot is finding over 250 new spyware programs, although only a minority of these are brand new, while the others are older versions with subtle changes made as an attempt to avoid detection. During 2004, Earthlink and Webroot collaborated to offer a free SpyAudit to Earthlink subscribers. From January 1, 2004 to September 27, 2004, more than three million scans were performed. The scans discovered approximately 83.4 million instances of spyware, for an average of 26 traces of spyware per SpyAudit scan. We will send the committee a copy of the 2004 year-end report once it is completed over the next week.

Industry analyst organizations like IDC are reporting similar findings. IDC's December 2004 report, "*Worldwide Spyware 2004-2008 Forecast and analysis: Security and System Management Sharing Nightmares,*" includes these findings:

- IDC estimates that 67 percent of all computers have some form of spyware, and in most cases, there are multiple spyware programs, even hundreds.
- The impacts of spyware go beyond annoying pop-ups and can be a serious drain on help desks and system management resources. The report estimates that in 2003 one or two out of every 100 support calls made by consumers concerned spyware. At the end of 2004, the estimate increased to two out of every five.
- Spyware is often a revenue source for legitimate corporations.

While the Committee has done an excellent job over the past year of articulating the many risks spyware and adware pose to individual computer users, little attention to date has been paid to the even more serious threat these malicious and unwanted programs can pose to larger organizations. When we consider the kinds of trade secrets, confidential government information, personnel and other sensitive data that can reside on computers used by corporations, government agencies and organizations, the economic costs and security risks associated with spyware are exponentially greater.

In the same IDC study mentioned above, they surveyed over 600 organizations, and found that spyware was the fourth greatest threat to a company's enterprise network security.

A survey of more than 275 IT managers and executives across the U.S. commissioned by Webroot in September, 2004 found some alarming results:

- Nearly 82 percent reported their desktops are currently infected with spyware, with more than a third noticing an increase in spyware infections in the previous six months.
- More than 70 percent of corporations expressed an increased concern with spyware.
- However, less than 10 percent of businesses have implemented commercially available anti-spyware software.

Between October 7, 2004 and January 1, 2005, Webroot's free and voluntary Corporate SpyAudit scanned more than 23,000 systems across more than 5,100 compa-

nies, and discovered an average of 17 pieces of spyware per corporate desktop computer.

A recent InformationWeek story entitled, "Another Fight to Wage," provides further evidence of these trends. The story, just published on January 17, 2005, reports the results from a survey of 400 business-technology professionals recently completed by its research department:

- Nearly 80 percent of respondents said their organizations have been infiltrated in the last 12 months by spyware.
- Over 70 percent will spend somewhat or significantly more money to manage spyware.
- Sixty percent will spend somewhat or significantly more money to manage adware.

THE ROLE OF GOVERNMENT

Webroot applauds the work of the Committee, your Senate counterparts and the Federal Trade Commission in publicizing the problems associated with spyware and other programs loaded on users' computers without their knowledge or informed consent.

We realize this committee, in particular, has spent countless hours trying to develop legislative language that will help offer consumers a higher level of protection and motivate regulatory enforcement actions against spyware purveyors.

The unfortunate reality is that there is no way to eradicate spyware through regulatory or enforcement means. The Internet is global, which makes establishing and enforcing legal standards very difficult. Just as large a challenge in this endeavor is the strong economic motivation that underlies the propagation of spyware and adware type programs, which is unlikely to be substantially diminished. As a further disincentive, we believe the bill should include criminal penalties, and we support the lack of a monetary cap in the enforcement section.

Given the growing prevalence of the problem, we support the legislation as a clear statement that these acts are covered under the law. In particular, many attempt to argue that arcane statements in small print buried at the end of lengthy end user license agreements constitute the notice and consent of the user. This is clearly not the case. Our number one priority is to advocate for our customers and to empower users with information they can use to make educated decisions about what enters their computers (and thus, their homes, companies and lives.)

To address this current problem, the bill sends a clear signal and sets a standard that deceptive practices cannot be used and that users must knowingly "opt-in" before software is loaded onto their computers. Along with these more stringent guidelines, increased awareness and public education about spyware is essential to effectively deal with the problem.

The "Good Samaritan" provision that is included is very important to help assure that companies like Webroot continue to exist and provide users with tools to find what is on their machines, and a means to remove things that users determine they do not want.

We also support the preemption provision of the bill. It is important that the law related to these practices be consistent throughout the U.S.

There are a few places where we are concerned that the bill language might not adequately cover the current practices we see. We would be happy to share results of our ongoing research efforts with the committee, to ensure that you have the most current information about the technology being used to invade computers, track users' activities without their knowledge, and undermine system security and personal privacy.

It is clearly going to take a combination of technology, public education, sound public policy and strong enforcement to address this problem. We are poised to offer any assistance the committee needs as you continue to work on this issue.

57

September 2004

Spyware, Supportware, Noticeware, Adware and the Internet

An Industry White Paper by the Information Technology Association of America

ITAA

Introduction

Spyware. The name sounds sinister, covert, perhaps even deceitful. Like agents in the real world, however, software programs operating in the background of an online session can be designed to conduct a helpful or harmful mission. The difference between "good" and "bad" software, therefore, is determined by the intent and behavior of those that develop and distribute the software, not interactive software technology itself.

This white paper explores the public's understandable confusion surrounding spyware, describes applications of the technology which are useful and beneficial as well as those that are problematic, even illegal; discusses how attempts to legislate or regulate spyware could introduce very negative unintended consequences for other types of interactive software; and delineates a set of public policy principles that must be upheld to assure that the online misbehaviors of the few do not harm the growth and diversity of Internet experiences for the many.

The Internet paradigm

In addressing how new forms of interactive technologies have been introduced and met with varying forms of acceptance by consumers, privacy advocacy groups and legislators etc., we should draw correct analogies to traditional commerce. These analogies help illustrate where existing laws and standards of conduct in commerce apply to the Internet.

For example, by engaging a website with a visit to one of its pages, is the consumer "entering the merchant's store physically," "making a phone call to them," or "responding to a mail order catalogue" or some mix of the above? By applying these metaphors, it becomes clear that, while no existing set of regulatory standards currently address all of the challenges raised by the implementation of interactive software, sufficient law already exists to combat the most serious concerns.

It is also crucial to understand that the Internet inherently calls for interactive software. Since the Internet facilitates communication, a software infrastructure needs to exist to support the transfer of information between users and computers. Long before the origin of the first Web browsers in the mid 1990s, interactive software was the underpinning of the Internet in the form of e-mail and file transfer protocols.

Since then, interactive software naturally has developed to meet the increased commercialized uses of the Internet. The once prevailing concept that the Internet would be used primarily for the free dissemination of information disregarded the costs of on-line publishing. As applications were developed to meet new demands, such as online weather and news, publishers needed a business model that would make information affordable.

Meanwhile, innovative Internet applications, such as instant messaging and Voice over Internet Protocol, depend upon interactive communications among user devices. These applications rely on "interactive dialogs" that allow devices to detect each other's presence.

Spyware vs. Supportware

Spyware is a broad category of software that operates without the knowledge, consent or control of the computer user. Spyware is introduced in a deceptive manner, performs functions that may be annoying or harmful, and, once loaded on a computer, can be difficult to eliminate.

Unfortunately, the term spyware has expanded over time to encompass other categories of interactive software that serve a useful purpose and are not deceptive, harmful or difficult to remove. This supportware may aid in the delivery of security services, support Internet access, facilitate a consumer's access to free software in exchange for viewing legitimate advertising messages, or perform other useful functions.

Spyware, however, poses a serious threat to the growth and vitality of the Internet. In a very real sense, the phenomenon could become to downloadable software and file sharing what spam has become to email. How bad is that? One study finds that nine out of ten emails received in the U.S. are spam.[1] Like spam, spyware developers use technology to behave in ways that go from merely annoying to downright criminal. For instance, it can be used to monitor a computer user's Web site visits, collect personally identifiable information and then misuse it. Some spyware, termed keyloggers, can capture keystrokes and be used to steal logins, passwords, credit card information or social security numbers.

The problem is particularly damaging to information security, both because this technology can be used to exploit vulnerabilities in legitimate computer software and because it can be used to block access to Web sites for security patches and upgrades. In the case of keyloggers, spyware is used to hijack browsers and other computer resources.

Propagation techniques for the technology can be particularly insidious. For example, spyware is often placed on file sharing networks in folders with names most likely to attract attention (like Britney Spears or Mariah Carey). And in some cases, spyware antidotes offered over the Internet as freeware can actually be spyware instead.

Spyware is not only deceptive, but prolific too. Unlike viruses or worms that generally attack a computer with a single file, this technology can plant thousands of files and change how a particular system is configured. The technology can also be designed to defend itself from removal. Files might work in tandem to replicate a destroyed partner. Designers also use random file

[1] Sharon Gauldin, "Nine Out of Ten US Emails are Now Spam," Datamation, June 8, 2004.

names and reshuffle file locations to make detection and removal more difficult.

Dell Computer reports that the problem has become the number one source of calls to its support centers, representing 12 percent of all technical support requests.[2]

The Consumer Software Working Group, a group of companies, organizations and individuals convened by the Center for Democracy and Technology have worked to describe examples of spyware and other unfair, deceptive and devious practices involving software. Their report is attached as Appendix A.

Adware

Adware is a separate variety of interactive software, which enables free and low-cost software and services by providing an economic rationale for providers.

Much of the free, downloadable software and services available on the Internet are no more free than programs broadcast on television networks. Traditional broadcasters are able to provide the programming at no charge to viewers because the costs for developing and delivering the programs are borne by commercial advertisers. In the same way, downloadable software and no-cost services such as instant messaging, P2P filesharing, multimedia players, music, games, file compression utilities and other capabilities are bundled with advertiser-supported adware. Consumers are asked to view banner ads and pop-up messages in exchange for access to the free or discounted product and service offerings.

It is important to note that consumers themselves may wish to receive the information contained in commercial messages as an assist to online shopping. Additionally, consumers often have the option of avoiding Web ads by opting for fee-based products and services.

The comparison of online and over-the-air advertising is not a perfect analogy. Unlike television advertising, adware often calls for the consumer to provide personal information. The advertiser uses this information to match advertising to the interests and buying habits of the consumer and to better understand the effectiveness of advertising investments. In practical terms, this sharing of online information is no different than the customer's willingness to fill out the warranty card information for a new product purchase or to provide details for a local merchant's mailing list.

Not unlike commercial television or a free newspaper, exposure to advertising is the implicit bargain that consumers strike when accessing content without paying for it. Adware facilitates that process, and in doing so makes content and service available to consumers for free or for a nominal cost.

---

[2] Maureen Cushman, Dell Computer, FTC Roundtable on Spyware

Noticeware

An additional type of interactive software can be called noticeware. Examples include spam filters, child safety filters, security warnings and virus alerts, and cookies, many of which are enabled by standards such as the Platform for Privacy Preferences (P3P) [3].

P3P is a specification that allows Web sites to publish standard, machine-readable statements of their policies for easy access by a user's browser. It automates the notification of Web site practices and can automate consumer choices regarding those practices.

The platform could also play an important role in technical efforts to enhance transparency and provide users with greater control over their personal information. It allows consumers to set general preferences regarding privacy policies in their browsers, which then communicate those preferences to Web sites. As a result, users can locate privacy policies easily, and Web sites can better inform users about their privacy policies and other practices.

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.

[3] The Platform for Privacy Preferences (P3P) (http://www.w3.org/P3P/)is a protocol developed by the World Wide Web Consortium,

Unintended Consequences of Legislation or Regulation

The continued growth of the information economy depends on providing consumers with tools to exercise their individual privacy rights and preferences, not foreclosing their technology options.

Existing law addresses most of the illicit behaviors of spyware makers:

- Title 5 of the Federal Trade Commission Act gives the US Federal Trade Commission the ability to take action against unfair and deceptive trade practices. This law applies in situations where a company acts in a deceptive manner in order to place a clandestine piece of software on an individual's computer;
- The Electronic Communications Privacy Act (ECPA) makes it illegal to intercept communications without a court order or permission of one of the parties. While this does not necessarily regulate collecting data from hard drive, it can stop the interception of what Web sites are viewed and click-thru data. This, however, only applies if the computer user has not agreed either through a EULA (end-user license agreement) or some other form of consent.
- The Computer Fraud and Abuse Act (CFAA) regulates programs that are spread by exploiting security vulnerabilities in network

software and that co-opt control of users' computers or exploit their Internet connection. CFAA applies especially to those programs that steal passwords and other personal information.

To the extent that current law does not address illicit spyware behavior, new legislation may be necessary. But caution should be the watchword in crafting anti-spyware measures. New laws should not target a class of technology, but a set of behaviors. Poorly designed legislative remedies could set in motion a variety of unintended consequences.

For instance, public policy must recognize the difference between enterprise networks and the public Internet. Organizations conduct a wide variety of activities over corporate networks, including the deployment of new software versions, security patches, and other upgrades. Rules designed to protect consumers and general computer users in the Internet environment may be counterproductive and even harmful in corporate network settings.

Proposals for spyware regulation sometimes fail to adequately reflect the characteristics of enterprise networks—computer networks owned by employers, but used by individual employees or students. For example should any notice and consent rights created by new legislation flow to the end users of enterprise networks or to the network owners?

The restrictions could limit the ability of network owners to use network management tools, as well as restrict their ability to update the programs on client machines with remote downloads of software upgrades.

Similarly, regulatory requirements for uninstall functions would apply to software that the owner of an enterprise network intends to operate on client systems. These requirements would make the distribution of authorized programs significantly more complex.

New laws could also interfere with the use of parental control software. Many families place smut filters and other technologies on their home computers to block access to Web sites with objectionable content. Laws making Internet tracking illegal could seriously hamper or destroy this worthwhile function. Similarly, laws that make uninstall functions so easy a child could do it—could produce exactly that outcome.

Laws that are too strict or overly broad could reign in the amount of content that is now provided for free on ad-supported Web sites. Such laws would undermine ad-supported business models and force content providers to move to fee-based services. That situation could, in turn, lead to a slow down or even a reversal of Internet growth.

Additionally, regulatory approaches that depend upon a consumer reading text based informational notices when entering a Web site or accessing content may not take advantage of the full potential of

Internet protocols such as P3P to empower consumers to exercise their own online preferences. Such online personalization can be a principle consumer benefit of Internet commerce, and the customization of consumer contact and ability to engage the consumer in an automated dialogue is a benefit inherent to the Internet itself.

Within enterprises and for individual consumers, substantial economies of scale are associated with distributing software via networks. An unintended consequence of an unduly burdensome regulation of network delivered software could be to discourage users from taking full advantage of security enhancing and productivity improving updates.

Conclusions: Combating Spyware; Protecting Principles

Spyware is clearly a threat to the online community. If not addressed, the spyware problem will grow both in terms of the volume of incidents and their severity. Computer users will grow increasingly frustrated with their online experience as system performance slows, settings and resources are hijacked, fixes become more difficult to obtain and apply, and privacy is increasingly invaded. This frustration could slow the popular adoption of broadband technology and the e-commerce marketplace generally. It could also have an extremely deleterious impact on Internet Service Providers, who may see their margins eroded as customer support inquiries in response to spyware concerns soar out of control.

At the same time, interactive software used in a constructive manner and serving useful social purposes can be important technology, facilitating the delivery of ad-supported content, extending parental control over objectionable materials, providing highly productive methods for software delivery and upgrade and performing other important roles.

So how can the technology be protected while wrongful behavior is controlled and corrected?

State legislatures are becoming increasingly aware of spyware as a public policy issue and have begun to respond to it. Unfortunately, as in the case of a law passed recently in Utah, attempts to reign in the use of spyware have muddied the waters for legitimate online service providers and e-commerce companies. The Utah law blurs the distinction between spyware and adware, undermines the ad-supported business model, and raises barriers for national merchants and service providers seeking to do business in the state.

ITAA believes that any approach to the spyware challenge must uphold the following principles:

Consent and Consumer Choice

To the maximum extent possible, consumers should be empowered to make their own privacy choices.

Individual privacy preferences vary greatly, so government regulation would be hard pressed to address the many variations of individual preference and computer sophistication. Meanwhile, the Internet marketplace has responded to consumer demand with a variety of tools that permit users to control their online experience.

For example, some proposals would apply a text-based "Clear and Conspicuous" notice standard to the Internet. As a standard for measuring font sizes in print advertisement, it belongs in a world where the publisher, not the consumer, determines how information will be displayed. This approach expects consumers to read and digest prospectus legal statements at each Web site they visit. It ignores the potential to far more effectively convey information to online consumers through Internet tools.

As previously discussed, more consumer-oriented notice standards would encourage the use of notice communications in machine readable protocols, letting the user preset computer preferences. Users benefit through adapting the advantages of technology, rather than imposing the standards of the print world that would generate more legislatively mandated pop-up notices. Giving users greater control over their online experience, ISPs, portals and other trusted sources can develop software screening processes to protect consumers from unwanted downloads, preventing malicious software.

Uniformity

In a networked economy, the exchange of information is an essential component of commerce. The interests of the Constitution's Commerce clause are served by having uniform national privacy rules. The inherently interstate nature of Internet commerce makes it essential that any legislative standard on Internet privacy be established on a nationwide basis. Any Federal legislation should therefore provide for Federal preemption of state law. The promise of the Internet economy cannot be realized with a cacophony of conflicting state laws.

Un-install

The workability of a statutorily required uninstall function is suspect, because it undermines the ability of enterprise owners to manage their networks. At the same time, the point of spyware is to deceive consumers and avoid detection. Therefore, mandated uninstall functions are unlikely to be effective in situations involving actual spyware and may instead create a false sense of confidence or security on the part of consumers.

Spyware legislation and regulation should focus on consumer harm, rather than limiting future innovation in the distributing of software. Similarly legislation should not prevent the bundling of software.

Enforcement

Penalties must be proportionate to actual consequences. Proposals for private rights of actions and minimum penalties raise the specter of trial lawyers using lawsuits to target Internet companies for even innocent mistakes. Damages for privacy violations should not be in excess of actual damages, or the benefit derived by the violator. Already Internet companies have been targeted by lawsuits with absurd theories:

- A trial lawyer in Texas sued Yahoo for $50 billion under the state's anti-stalking law for using cookies.
- A major law firm specializing in class actions sued two Internet companies because they "violated" the Federal Electronic Communications Privacy Act and the Computer Fraud and Abuse Act by placing cookies on the hard drives of consumers' computers.

Like its name suggests, spyware exists in a murky area in law, technology and popular understanding. While its harmful consequences are not as thoroughly appreciated as computer viruses or network attacks, the potential for harm caused by the use of this technology is formidable and growing. Spyware developers have begun to leverage the techniques of virus writers and other bad actors. This convergence hints at a witches' brew of future problems for Internet users. As spyware proliferates, the promise of the Internet shrinks. And the anxieties associated with this issue may spread to any type of freeware, shareware or downloaded software.

The prospects are sobering. The time for concerted industry action is now.

About ITAA

The Information Technology Association of America (ITAA) provides global public policy, business networking, and national leadership to promote the continued rapid growth of the IT industry. ITAA consists of over 350 corporate members throughout the U.S., and a global network of 60 countries' IT associations. The Association plays the leading role in issues of IT industry concern including information security, taxes and finance policy, digital intellectual property protection, telecommunications competition, workforce and education, immigration, online privacy and consumer protection, government IT procurement, human resources and e-commerce policy. ITAA members range from the smallest IT start-ups to industry leaders in the Internet, software, IT services, ASP, digital content, systems integration, telecommunications, and enterprise solution fields. For more information visit www.itaa.org.

Appendix A

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 underinclusive in important respects or, more commonly, overbroad so that they include practices that clearly benefit consumers, or both.[1]

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 consumerfriendly counterparts when carried out with proper notice and consent and in ways that give consumers

[1] 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.

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 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
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[2]
TRUSTe
Webroot Software
WhenU
Yahoo!

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

○