S. HRG. 108–1002

S. 2145, "THE SPY BLOCK ACT"

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMUNICATIONS

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

MARCH 23, 2004

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PUBLISHING OFFICE

20–672 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

JOHN MCCAIN, Arizona, *Chairman*

TED STEVENS, Alaska
CONRAD BURNS, Montana
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
SAM BROWNBACK, Kansas
GORDON H. SMITH, Oregon
PETER G. FITZGERALD, Illinois
JOHN ENSIGN, Nevada
GEORGE ALLEN, Virginia
JOHN E. SUNUNU, New Hampshire

ERNEST F. HOLLINGS, South Carolina, *Ranking*
DANIEL K. INOUYE, Hawaii
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
JOHN B. BREAUX, Louisiana
BYRON L. DORGAN, North Dakota
RON WYDEN, Oregon
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK R. LAUTENBERG, New Jersey

JEANNE BUMPUS, *Republican Staff Director and General Counsel*
ROBERT W. CHAMBERLIN, *Republican Chief Counsel*
KEVIN D. KAYES, *Democratic Staff Director and Chief Counsel*
GREGG ELIAS, *Democratic General Counsel*

SUBCOMMITTEE ON COMMUNICATIONS

CONRAD BURNS, Montana, *Chairman*

TED STEVENS, Alaska
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
SAM BROWNBACK, Kansas
GORDON H. SMITH, Oregon
PETER G. FITZGERALD, Illinois
JOHN ENSIGN, Nevada
GEORGE ALLEN, Virginia
JOHN E. SUNUNU, New Hampshire

ERNEST F. HOLLINGS, South Carolina, *Ranking*
DANIEL K. INOUYE, Hawaii
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
JOHN B. BREAUX, Louisiana
BYRON L. DORGAN, North Dakota
RON WYDEN, Oregon
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington

CONTENTS

WITNESSES

S. 2145, "THE SPY BLOCK ACT"

TUESDAY, MARCH 23, 2004

U.S. SENATE,
SUBCOMMITTEE ON COMMUNICATIONS,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:30 p.m. in room SR–253, Russell Senate Office Building, Hon. Conrad Burns, Chairman of the Subcommittee, presiding.

OPENING STATEMENT OF HON. CONRAD BURNS, U.S. SENATOR FROM MONTANA

Senator BURNS. We will call the Committee to order. Thank you for coming today as we look at another problem we face in the world of Internet. In the world of worms and viruses, you'd think this would be the Ag Committee but it's not. Cookies and implants, you can put that it in any committee. But today's hearing concerns a topic of critical importance to the future of consumer privacy and electronic commerce in the digital age, and I refer to the flood of spyware, which has been increasingly burrowing itself into consumers' computers, often without their knowledge.

I'm pleased to benefit from the hard work and expertise of my friend, Senator Wyden. We've worked together on many issues and I look forward on working with him on this one. We passed CAN SPAM, which after 4 years finally became law, and we may be a little bit ahead of the curve whenever we start talking about the subject that we're visiting about today. I'm convinced that spyware is potentially an even greater concern than junk e-mail, given its invasive nature.

I appreciate the support of another one of my colleagues on the Committee who has been an ardent defender of consumers' rights online, and of course, that's Senator Boxer of California. Together we have crafted legislation aimed at ending the insidious operation of spyware, and it is the SPY BLOCK Act of 2004.

Spyware refers to the software that is downloaded onto users' computers without their knowledge or consent. It's a sneaky way of software that is often used to track the movements of consumers online and even steal passwords. The porous gaps of spyware creates in a computer's security may be difficult to close.

For example, one popular peer-to-peer file sharing network routinely installs spyware to track users' information and retrieves targeted banner ads and pop-ups. As noted by the recent article in *PC Magazine,* these file sharing networks may be free, they may be free but at the cost of privacy and not money.

Of the 60 million users, few know that they are being watched, and those who discover spyware, uninstalling it may prove to be difficult other than the software programs. Some spyware includes tricklers. Now we've got a new word in vocabulary now, tricklers, which reinstall the files as you delete them. Users may think that they are getting rid of the problem, but the reality of the situation is far different.

So creators of spyware have engineered the technology so that once it is installed on a computer, it is difficult and sometimes impossible to remove, in some cases requires the entire hard drive to be erased to get rid of the poisonous product. Such drastic measures may be taken, because often spyware tells the installer what websites the user visits, it steals the passwords or other sensitive documents on a personal computer, and also redirects Internet traffic through certain websites.

One of the most disturbing aspects about the spyware problem is that so few consumers are aware of it. Bearing this in mind, the SPY BLOCK bill relies on a common sense approach, which prohibits the installation of software on consumers' computers without notice, consent, and reasonable uninstall procedures. The notice and consent approach which SPY BLOCK takes would end the practice of so-called drive-by downloads, which some bad actors use to secretly download programs onto users' computers without their knowledge.

Under SPY BLOCK, software providers must give the consumers clear and conspicuous notice that a software program will be downloaded in their computers and requires user consent. This simple provision could be fulfilled by clicking yes in the dialogue box, for example.

SPY BLOCK also requires notice and consent from other types of software. In the case of adware, another here we got, providers are required to tell consumers what types of ads will pop up on the users' screens and at what frequency. Consent is required for software that modifies user settings or uses distributed computing methods by utilizing the processing power of individual computers to create larger networks.

And finally, software providers must allow for their programs to be easily uninstalled by users after they are downloaded. As with CAN SPAM law, enforcement authority would be given to the Federal Trade Commission. The state's attorney general would also take action against purveyors of spyware, and it also empowers the users.

Clearly, the right balance must be reached between punishing bad actors and not impeding legitimate e-commerce. I am open to discussing with my colleagues ways to craft this legislation as to capture the truly malicious offenders. Make no mistake about it. The intent of SPY BLOCK is to bring back a little truth in advertising. Clearly, accountability needs to be brought to bear on this issue.

I'm anxious to hear exactly how using the unique brands of trusted companies to redirect consumers to their commerce sites is a legitimate business practice. While I understand this may be explained as a high-tech form of contextual marketing, I am very

leery on the broad types of questionable business practices that could be legitimized by this line of thinking.

Working closely with my good friends, Senator Wyden and Senator Boxer, I'm confident that we can make major progress on this legislation before spyware infects a critical mass of computers and renders them useless. Just trying to keep up with the latest anti-spyware software imposes a tremendous cost to business, let alone individuals who have to spend their time online worried about the next spyware infestation.

I look forward to hearing the testimony today and I appreciate our witnesses, and now Senator Wyden. And thank you so much for your good help.

STATEMENT OF HON. RON WYDEN,
U.S. SENATOR FROM OREGON

Senator WYDEN. Thank you, Mr. Chairman. It's great to have a chance to team up with you. I think once again we're showing that work in this area clearly can be bipartisan and we have gone this way on a host of initiatives. It's great to team up with you and then, of course, to have Senator Boxer, who's such an articulate and strong advocate, not just of consumers, but the technology sector. To have her with us as well is a great pleasure.

You said it very well and I'm just going to make a couple of quick comments. In fact, Mr. Chairman, if I could, I've got a longer statement and I'd like to have that placed in the record.

Senator BURNS. Without objection.

Senator WYDEN. Mr. Chairman, it just seems to me what is going on here is that snoops and spies are really trying to set up base camp in millions of computers across the country, and what we are in effect saying is that the owners of computers in this Nation ought to have control over what software gets placed on that computer. It really is just that simple. That really belongs to the computer user, and so what you have is in effect all these sneak, covert kinds of programs that are really trying to take those rights away from the owners of computers around the country. It seems to me that this will ensure that computer owners have knowledge and control over what gets placed on their computers, and given the sophistication of people who try to take advantage of the public, it seems to me that this is important legislation to move on now.

In effect, what these individuals who are engaging in this activity that we think is violative of the computer owners' rights, what they are doing is they're acting as parasites, they're acting as people who would put parasites on computers, put unwanted software that can burrow in and install itself on a hard drive where it proceeds to use the computer and the Internet connection for its own purposes. And as you have noted, the owner of the computer frequently doesn't know the intruder is there and very often has no way to get rid of it once he or she finds out.

So I think as we go forward in this debate, for those who may have reservations about this and want to oppose it, I want them to answer the central question. How can it be that those who own computers and have access to the Internet shouldn't have that treated as private property? That is what this is really all about. You don't get opportunities to come into somebody's home without

their knowledge and permission, and you shouldn't expect others to be able to take advantage of you in the kind of way that these parasites and snoops and spies are doing.

I think we've written this bill carefully. I'd like to put into the record an editorial from the *New York Times* that I think makes an important point in the sense that it's important not to write the definitions of what we're going to be doing to protect the consumer in too narrow a fashion. The Center for Democracy and Technology has done some very good work in terms of trying to ensure we have enough flexibility in those definitions so as to address the issue in a responsible way, and I'd very much like to have the editorial from the *New York Times* warning about the danger of making sure that you don't write this bill in too narrow a fashion put into the record.

I think this is a good bill and the fact that you and I and Senator Boxer have a chance to team up on it means that we can make this a priority even though this session is short, and I hope that we will be able to move it quickly to the full committee.

Senator BURNS. Thank you, Senator Wyden, and I do too. I share your concerns. It's my computer, it is private property, I bought it and paid for it, and for my use only, not some leech. Senator Boxer.

STATEMENT OF HON. BARBARA BOXER,
U.S. SENATOR FROM CALIFORNIA

Senator BOXER. Mr. Chairman, I couldn't top that, I really couldn't. I am so pleased to work with you and Senator Wyden and our staffs have worked together and I'm proud to be on the SPY BLOCK Act, and I'd ask unanimous consent that my full statement be placed in the record.

Senator BURNS. Without objection.

Senator BOXER. And I will summarize it very briefly. If we saw someone with a binoculars looking in someone else's window, we'd call the cops, and I think that in many ways what we're doing is very similar to that, but it's even worse than looking in a window. It's really getting into someone's head and someone's life.

So this is really important, it's very important, and I do hope we can prevail and get this done pretty quickly. You know, it is a pro-consumer bill, but I want to say to my colleagues it's also a pro-industry bill in my opinion. We're going to have people say it isn't, but it is, because I got news for you. If people think that they're being spied upon, they're going to use that computer a lot less than they normally would, and we're going to have people running away from using their computer just because this is America and we don't like that.

So I think what we're doing is pro-consumer but it's pro-business as well. And basically the rest of my statement goes into how it's very important to clearly talk about software, not just spyware, and that's what we try to do in the bill so people can't say, well, my definition doesn't fit to what you're doing. We want to make sure we cover everybody and that this bill is really going to do the job that it set out to do.

So again, I'm very pleased to be with you in this fight and I hope we can get it done. And I'm going to be running out for a minute and coming back to hear the testimony and look forward to our partnership on this.

[The prepared statement of Senator Boxer follows:]

PREPARED STATEMENT OF HON. BARBARA BOXER, U.S. SENATOR FROM CALIFORNIA

Mr. Chairman, thank you for holding this hearing. Last month, I joined you and Senator Wyden in introducing the "SPY BLOCK Act" (S. 2145). Our legislation is designed to address increasing concerns that I have heard coming from California and other states over "spyware."

Spyware, and other types of software called "Adware," are delivered into the homes and offices of consumers and onto their computers often without their knowledge and consent.

These invisible snoops follow consumers everywhere they go on the Internet and they bombard consumers with targeted pop-up ads.

Our bill simply says that software makers, including spyware makers, cannot sneak into your computer. Specifically, the SPY BLOCK Act prohibits the installation of software without notice and consent of an authorized user. Additionally, the software must provide clear procedures to uninstall the software and must be capable of being completely and easily removed.

The most common objection to the bill we have heard is that it should focus only on "spyware." But as this hearing will show, nobody thinks the software they produce IS spyware.

The reason the legislation targets software is because the people who produce spyware will always try to define themselves out of the category by claiming that their particular software is not spyware. By applying common principles of consumer rights for all software, we deal with the spyware problem and enhance consumer rights on the Internet more broadly.

Mr. Chairman, I am proud to work with you on this issue and look forward to working with the witnesses here today to make the legislation as effective as possible.

Senator BURNS. Thank you, Senator Boxer. We'll keep you up to date.

Senator BOXER. I'll be right back.

Senator BURNS. OK. We'd ask our witnesses to come to the table now. We have Mr. Avi Naider, President and CEO of WhenU.com Inc. from New York; Mr. Robert Holleyman, President and CEO of Business Software Alliance, we worked a lot with that group of people and with extreme pleasure; Mr. Jerry Berman, President of the Center for Democracy and Technology, and, of course, if there has been a man who has been around the Internet any longer than this man then they had to come before dirt almost, Jerry, so thank you for coming today.

Mr. BERMAN. Are you talking about my age or my expertise?

Senator BURNS. Both, I think. And Dr. John Levine, President and CEO of Taughannock Networks from up in New York, and we appreciate you coming today too and I'll try and get that networks pronunciation down much better so I'll have to apologize for that.

We'll start with you, Mr. Naider, if you're ready, and we look forward to hearing your testimony.

STATEMENT OF AVI Z. NAIDER, PRESIDENT AND CHIEF EXECUTIVE OFFICER, WHENU.COM, INC.

Mr. NAIDER. Good afternoon, Mr. Chairman and Members of the Subcommittee. I thank you for the opportunity to appear before your Subcommittee as it examines the issues surrounding spyware. I am Avi Naider, President and Chief Executive Officer of WhenU.com. WhenU is an online contextual marketing company. WhenU makes software that recognizes the immediate interests of an online consumer and automatically displays highly pertinent

coupons and advertisements in response to the consumers' expressed interest.

Consumers visiting the Staples website who have WhenU software might be presented with a coupon to save $30 off a $150 purchase at Staples. Consumers researching a trip to London who have WhenU software might be shown a pop-up with a special $99 fare on British Airways. This is why we named the company WhenU. It provides you with relevant and timely information when you shop online, when you travel to London, and so on.

Our software presents information to consumers that is targeted and timely. At the same time, our software aggressively protects consumer privacy. In the past, targeted marketing in the U.S. has been enabled by collecting information about households and individual consumers into large data bases. These data bases are replete with information about who we are, what we buy, how affluent we are, and lots of other personal information.

We started WhenU because we believe that targeted marketing can be done without collecting personal information about consumers and building profiles. WhenU does not have a database of consumers or any consumer profiles at all. Instead, our software uses a proprietary directory of the Internet that categorizes various indicators of consumer interest and delivers precisely targeted messages that inform the consumer's decisionmaking process.

The software does all this without sending individual consumer activity back to WhenU. WhenU's software-based advertising is a promising technology that begins to fulfill the potential of the Internet as a rich, personalized, one-to-one marketing and information delivery experience. We believe that WhenU software and other methods of contextual marketing are likely to emerge as engines of major growth for the Internet in the future.

The WhenU desktop advertising network represents millions of consumers who have installed WhenU software on their computers. Typically, consumers download WhenU contextual marketing software as part of a bundle that contains free popular software. Developers of such free software rely on the revenue generated by companies like WhenU often as their sole or primary revenue model. They view WhenU as win-win technology that offers consumers free coupons, relevant advertising, and free software, all while protecting consumer privacy.

WhenU software is anything but spyware. WhenU follows a strict privacy policy, and in addition, respects the principles of consumer choice in the following ways. The consumer always receives a clearly visible notice that WhenU software is part of a download. The consumer is given easy access to a clear and concise license agreement that he must affirmatively accept to proceed with the installation of WhenU software.

WhenU-generated ads, offers, and coupons are boldly and conspicuously branded by WhenU, and WhenU software is easy to uninstall. WhenU fully supports the principles underlying the SPY BLOCK Act. We also favor further and detailed study of the complex issues presented in order to enable Congress to craft an effective national legislative solution.

Many of the legislative issues currently proposed, both at the state and the Federal level, are either overly broad or lack the nec-

essary nuance to address the problem effectively, and yet still allow promising technology to develop. As a result, they potentially regulate or even restrict consumer-friendly, privacy-protective, and mainstream software, while failing to protect consumers against software that truly threatens privacy and security.

Ironically, carelessly-worded spyware legislation that lacks nuance will do more to promote the spyware problem than solve it. Because if legitimate advertising models that truly give choice to consumers are lumped in with nefarious software that intends to deceive, rogue and unscrupulous companies who play by no rules and adhere to no standards of consumer protection will be given the upper hand in the marketplace, and this outcome would be devastating.

On the other hand, carefully worded and nuanced legislation can set standards for the online industry and serve as a beacon for the marketplace and for advertisers looking to use legitimate technologies that can reach their target consumers. We believe that the proceedings today and the FTC workshop to be held in April will produce a detailed record that will undoubtedly help inform future legislative efforts.

We look forward to continuing to work with you, Mr. Chairman and the members of the subcommittee to develop a comprehensive and effective solution to this pervasive problem. Thank you.

[The prepared statement of Mr. Naider follows:]

PREPARED STATEMENT OF AVI Z. NAIDER, PRESIDENT AND CHIEF EXECUTIVE OFFICER, WHENU.COM, INC.

Introduction

Good afternoon, Mr. Chairman and members of the Subcommittee. I thank you for the opportunity to appear before your Subcommittee as it examines the issues surrounding "spyware." I am Avi Naider, President and Chief Executive Officer of WhenU.com, Inc. ("WhenU").

WhenU and the Evolution of Contextual Marketing on the Internet

WhenU is an online contextual marketing company. Our software delivers information about products and services to consumers online at the moment that information is most relevant to them. WhenU addresses an age-old problem: consumers' lack of access to potentially valuable market information when they need it most. Although consumers are inundated on a daily basis with information of all sorts, including offers from advertisers, the value of such information is reduced because it is not shown to the consumer at the right moment in time. WhenU's software delivers highly pertinent coupons and advertisements based on consumers' immediate interests, as reflected in their immediate Internet browsing activity, yet is highly protective of consumer privacy.

Contextual marketing technology as developed by WhenU evolved naturally from the decades old, multi-billion dollar database marketing industry, which at its core, relies on behavioral targeting of consumers. Database marketing has been used for years by numerous companies to analyze individual consumers' past purchasing behavior in an attempt to determine what discounts and offers would be most attractive to those consumers in the future. For example, American Express tracks and analyzes the purchasing behavior of its credit card holders and uses the information gleaned from such analysis to mail potentially pertinent offers to such consumers.

More recently, companies have advanced the field of behavioral marketing by deploying new technology-driven solutions. For instance, Catalina Marketing has developed technology that links to the point-of-sale (POS) systems of many grocery stores and analyzes the purchases of individual consumers as they are scanned by the cashier. Based on the particular products purchased by the consumer, targeted offers and incentives for competing products are then immediately printed for the consumer (typically on the back of his or her grocery store receipt).

Software-based contextual marketing technology as developed by WhenU is a further evolution in the field of behavioral marketing. Whereas traditional database

marketing companies, and even innovators such as Catalina Marketing, analyze a consumer's past and current purchases to predict what the consumer will purchase in the future, software-based online marketing technology assesses the activity of the consumer in real time, at the very moment the consumer is researching a certain product or category of products on the Internet. Essentially, WhenU's technology utilizes the unique capabilities of the Internet environment to offer the consumer information that might assist him or her in making a purchase decision before the decision is made, at a time when the information is most useful. Imagine that while you are looking in a store window at a new DVD player, someone approaches you with an offer to get a DVD player at a better price at a store down the street. WhenU's technology allows the same thing to happen millions of times per day by providing consumers with offers to purchase all types of goods and services on the Internet.

The Internet by its very nature enables real-time contextual marketing in a robust and scalable manner. Since the Internet is a medium in which all activity is transmitted electronically, WhenU software can scan the Internet browsing activities of a participating consumer to determine his or her immediate interests, and connect thousands of advertisers and millions of participating consumers with the right advertisement or coupon when it is most relevant to the consumer. WhenU's software effectively provides consumers with comparative advertising that presents them with a choice. The idea behind the WhenU software was to revolutionize targeted marketing from the old model in which interests are deduced based on who a consumer is and what their personal information is, to a new software-based system that focuses on actual interests as reflected in their Internet browsing activity-when you shop, when you travel, when you invest. In fact, that's why we named the company WhenU. "When you" are about to book a trip to London, WhenU software will deliver a relevant offer to you.

Best of all, WhenU is able to deliver precisely targeted advertisements that are highly relevant while at the same time protecting consumer privacy. From the beginning, consumer privacy has been important to WhenU. WhenU does not collect any personally-identifiable information. The WhenU software does not track user data, does not use cookies to track consumers, does not track users' clickstream data, does not create anonymous user profiles, and does not compile a centralized database of users. All of the activity takes place on the user's computer (or "desktop"). The only information that is transmitted back to WhenU is information that allows us to show advertisements and coupons to the consumer and make sure the offers we do show are shown at the moment that they are likely to be most useful to the consumer. We are proud of our privacy policy and explain it in detail on our website.

WhenU's software represents a significant departure from the way advertising online initially started. In general, early methods of online advertising were not able to deliver on the promise of the Internet as a rich, personalized consumer contact point. Poorly targeted e-mails, banner ads, and non-contextual pop-ups have yielded click through rates of less than one percent (1 percent), and millions of wasted advertiser dollars. To leverage the full power of the Internet and continue to develop the Internet into the kind of rich revenue-generating medium it should be, advertisers have begun to understand that successful online advertising must take advantage of the Internet's unique potential to deliver targeted and relevant advertising in response to what consumers are looking for.

As an example, paid online search, a model promoted currently by companies such as Yahoo! and Google, represented as little as 3 percent of the online advertising market in the year 2000, but this year is expected to reach 37 percent as advertisers recognize the power of delivering relevant ads to consumers seeking specific products. When U believes that software-based advertising will similarly emerge as an engine of major growth for the Internet in the future, as advertisers and consumers continue to experience the power and richness of software as a medium for delivering highly targeted and useful information and advertising online.

WhenU's Desktop Advertising Network

The WhenU Desktop Advertising Network represents millions of consumers who have installed the WhenU software on their computers. Typically, consumers download the software as part of a package, or "bundle," of software that enables consumers to get popular software for free. Software companies routinely bundle revenue-generating, advertising software (known as "adware") with free software programs (known as "freeware") to enable them to offer the freeware to consumers at no cost. In some instances, software developers might give consumers the choice between paying for the software or agreeing to receive ads from WhenU in exchange for getting the software for free. Developers of such free software applications rely

on the revenue generated by software companies like WhenU to enable them to continue to offer their software free of charge. In any event, consumers are given a clear notice and choice whether or not to download WhenU software.

Once downloaded, the WhenU software (called SaveNow, or Save!, but referred to generally as SaveNow) resides on the consumer's computer and generates advertisements through the use of a proprietary directory that is delivered to and saved on the consumers' desktop when the consumer installs the software. This proprietary directory is compiled and updated by categorizing the Internet in much the same way as a local Yellow Pages indexes merchants into various categories.

As a participating consumer "surfs" the Internet, the SaveNow software studies page content, keywords, web addresses, and search terms from the consumer's web browser to determine whether any of those terms, web addresses and/or content match the information in the directory. If the software finds a match, it identifies the associated product or service category and determines whether an appropriate advertisement for that category is available to be displayed, subject to timing and frequency restrictions contained in the software.

With the WhenU software, it is ultimately the consumer who drives whether a particular element will be included in the WhenU directory, because the directory is intended to contain terms that reflect the interests of the consuming public. Similarly, it is the user's actions on his or her desktop that ultimately determine whether an advertisement is eligible to be seen. Since its founding in February 2000, WhenU has delivered online marketing for more than four hundred advertisers, including such well known companies as Priceline, British Airways, Delta Airlines, JPMorgan Chase, Kraft, Cingular, Ford, and ING Bank.

In short, WhenU provides a useful and privacy-protective opt-in service to participating consumers, provides a revenue model for popular free software, and contributes to the development of the Internet-enabled desktop as a comparative shopping medium.

What is Spyware?

"Spyware" generally refers to software that appears harmless but, once downloaded, operates differently than its stated functionality, such as by stealing or transmitting personal data about the consumer and his or her browsing habits, keystroke data, or clickstream behavior. Spyware also can refer to software that sneaks onto user's computers, masks its operations once it has been installed on the computer, and is nearly impossible to uninstall. Sometimes programs that are surreptitiously downloaded onto user's computers and show ads whose source is not easily identifiable are referred to as spyware.

WhenU has sometimes been accused of being "spyware." It is not surprising that some people who do not understand the WhenU technology think that it is invasive to privacy how else, they wonder, can it alert a consumer to a discount hotel site when that consumer is looking at hotel rates in Washington, D.C.? However, properly understood, WhenU's unique proprietary technology cannot be considered spyware. WhenU's software-based advertising model respects the principles of consumer choice and consumer privacy, in three distinct ways.

First, regardless of the method of distribution, during the installation process, the consumer always receives a prior notice that SaveNow is part of the download. To proceed with the installation of SaveNow, the consumer must affirmatively accept a clear and concise license agreement. The license agreement explains that the software generates contextually relevant advertisements and coupons, utilizing "pop-up" and various other formats.

Second, once a user has installed the SaveNow software, it is easy for a user to identify what the WhenU software does. WhenU makes the ads, offers and coupons served by WhenU easy to identify. Ads on the WhenU Desktop Advertising Network are displayed in a separate, WhenU-branded window, including the marks "Save!" or "SaveNow", depending on the particular download partner, and other elements specially included in the WhenU window. In addition to WhenU's unique branding, every WhenU offer also contains a notice on its face that: "This is a WhenU offer and is not sponsored or displayed by the websites you are visiting." And, with WhenU's highly-protective privacy policy, users do not have to be concerned about privacy, since no personal information is transmitted to or collected by WhenU. In fact, WhenU's strict privacy policy far exceeds current standards in the Internet advertising industry.

Finally, after accepting a license agreement and downloading the software, consumers can easily remove or "uninstall" the software from their computers if they no longer wish to keep it. Every ad shown by WhenU contains inks to further information about the software and information about how to uninstall it. In addition, these links also allow consumers to easily contact WhenU by e-mail for more infor-

mation. The software can be easily uninstalled through the computer's Control Panel Add/Remove Programs menu, the standard process used for uninstalling most Windows-based software. Once properly uninstalled, the WhenU software will cease to operate or show advertisements or coupons on the consumer's computer.

The Threat of Spyware and the Solutions to Spyware

Spyware is a serious problem affecting millions of computer users every day. If the spyware problem continues to grow, unabated, it may deter computer users from the Internet and slow the creation and dissemination of new and innovative software programs available to users from the Internet.

As discussed above, WhenU is very different from "spyware." But notwithstanding these significant differences, WhenU is often swept in with software that threatens user security and privacy. That is why we believe that it is necessary and desirable for Congress and the FTC to regulate this area in order to protect consumers from spyware and protect the development of the Internet as a rich and promising medium.

Current efforts being employed to address consumer concerns are helpful, but they typically fail to get at the real problems presented by spyware. For instance, the marketplace is replete with "anti-spyware" software, but many of these software programs are indiscriminate in their identification of so-called "spyware" and, as a result, often identify benign programs or even files such as cookies, which are commonly employed by Internet websites to identify users who have accessed the site previously. Moreover, most of these programs prompt users to uninstall any software identified as spyware or as a threat. As a result, consumers may be prompted to unknowingly uninstall software that is far from nefarious and that they or another member of their household quite deliberately installed. Users may even have paid for software they are prompted to uninstall, or they may be required to keep such software to support free software that they have also installed. If marketplace solutions unduly burden the revenue model that software providers rely on to continue to offer their software for free, it will discourage the creation and distribution of free software, and force consumers to have to pay for such programs.

At the same time, State legislative solutions are being proposed to respond to the growing menace of spyware, but many of these proposed solutions suffer from the same problems created by "anti-spyware" software: They inadvertently regulate or even restrict consumer-friendly, privacy-protective and mainstream software while failing to protect consumers against software that truly threatens consumer privacy and security. They are also subject to the concerns of local businesses and may not address the problem from a national perspective. As a consequence, these solutions, such as the one recently proposed and passed by the legislature in Utah, are generally ineffective and overly broad.

WhenU is in favor of Federal efforts to combat spyware, and fully supports the principles behind the SPY BLOCK Act. As per our practice, WhenU believes that users should receive notice about any application before they download it, should be required to affirmatively accept a clear license agreement that discloses the nature of the application and its functionality, should be presented with information that identifies the source of every window that is generated by software on their desktop, and should be able to uninstall any software application through standard and easily accessible means. WhenU also is in favor of legislation that provides that the Attorney General, States Attorneys General and the FTC should be solely responsible for implementing and enforcing its provisions. However, WhenU first supports careful study and consideration of the problems surrounding spyware. How to combat "spyware" is a complex issue, and we believe the approach lawmakers should take to address the issue should be as nuanced as the problem itself.

Ironically, carelessly worded spyware legislation that lacks nuance will do more to promote the spyware problem than solve it. If legitimate advertising models that truly give choice to consumers are lumped in with nefarious software that intends to deceive, rogue and unscrupulous companies who play by no rules and adhere to no standards of consumer protection will be given the upper hand in the marketplace. And this outcome would be tragic. On the other hand, carefully worded and nuanced legislation can set standards for the online industry and serve as a beacon for the marketplace and for advertisers looking to use legitimate technologies that can reach their target consumers.

We believe that the proceedings today and the FTC Workshop to be held in April will produce a detailed record that will undoubtedly help inform future legislative efforts. We look forward to continuing to work with you, Mr. Chairman, and the members of the Subcommittee, to develop a comprehensive and effective solution to this pervasive problem. Thank you.

Senator BURNS. Thank you very much. Robert Holleyman, thank you for coming today, Software Alliance.

STATEMENT OF ROBERT W. HOLLEYMAN II, PRESIDENT AND CEO, BUSINESS SOFTWARE ALLIANCE (BSA)

Mr. HOLLEYMAN. Mr. Chairman, Senator Wyden, it's indeed a pleasure to be here this afternoon testifying on behalf of the member companies of the Business Software Alliance. Our organization works for leading developers of personal computer software, enterprise software, our key hardware partners and Internet technology developers on public policy issues in the United States, where we're headquartered, and in more than 65 countries around the world.

I am delighted to be able to talk with you today about options to provide the best way to protect consumers from the problems associated with spyware. At the Business Software Alliance, we applaud the intent of the SPY BLOCK Act that you have introduced along with Senators Wyden and Boxer.

This afternoon I'd like to make three key points. First, computer snooping or spying on computer users is reprehensible behavior that invades our privacy. However, the problem is with bad behavior, not bad software tools or products.

Second, for this very reason, Congress should ban only the behavior and not the technology. And third, we believe that the bill as introduced can be enhanced by focusing more directly on punishing such behavior. Doing so would accomplish the current intent of the bill without placing Congress in the position of approving or disapproving technologies.

Indeed, Mr. Chairman, you and the other Members of this Committee have been leaders in adapting laws to the information age. You've done so carefully, deliberately, and in a well thought out fashion. We agree fully that we need to stop e-spying and that it will harm the consumer experience in using their computers and the Internet. It is wrong and it should be stopped.

But it's also essential that we recognize that the problem comes from bad people, bad actors, not from bad products. That same underlying technology that can enable spyware also may power many legitimate applications that benefit millions of computer users every day.

Mr. Chairman, I feel like I'm preaching to the choir. Last year Congress stopped unwanted telemarketing, not telephones. You canned SPAM by criminalizing fraudulent conduct, not by banning commercial e-mail. And in the 1990s, you wisely recognized it was unwise to try to ban encryption technology, choosing instead to focus on those who might use encryption to commit crimes.

Your Committee and the Congress as a whole has wisely and consistently avoided technology mandates. You understand that the U.S. technology industry and our own leadership in high-tech innovation are crucial to America's economic future.

We appreciate the author's clear intent to protect legitimate software from being swept into the bill and you've done so through a series of definitions and exceptions that the bill employs. However, at the same time, the BSA feels that these definitions can be fraught with peril in the current software environment, especially as new technological developments occur.

As an alternative, we suggest that the Congress focus on the most egregious practice of commercialization of information from electronic spying. Congress should prohibit the distribution of user information obtained electronically from an individual's computer unless one of two tests are met. Either the person seeking to sell the information must show that it was collected with the user's permission or that it was obtained from an entity that collected the information with such permission.

Such an approach would achieve the main objective of stopping e-spying while significantly avoiding the tough definitional issues and their implications for the future development of technology.

With respect to enforcement, we agree that the FTC should be given primary responsibility. The FTC should treat violations as an unfair or deceptive activity under the FTC Act. We also believe that the Justice Department should be authorized and empowered to subject those who violate the legislation to criminal fees and imprisonment under Title 18 of the United States Code. That would send a clear message that the commercialization of information from electronic spying will not be tolerated.

However, we think that state attorneys general should be given enforcement authority in this area only if we have a Federal standard. Remote access electronic spying through spyware is a national problem and we think it should be treated as such.

I'd like to thank you again, Mr. Chairman, for the opportunity to talk today on the issue of spyware and the SPY BLOCK bill. We believe that working together this bill can be enhanced to directly and effectively address the issue we're all most concerned about, electronic spying. The BSA is eager and willing to work with you and the other members of the Committee in that regard, Mr. Chairman. Thank you for this opportunity to testify.

[The prepared statement of Mr. Holleyman follows:]

PREPARED STATEMENT OF ROBERT W. HOLLEYMAN II, PRESIDENT AND CEO, BUSINESS SOFTWARE ALLIANCE (BSA)

Good morning. Thank you very much for the opportunity to testify here today. My name is Robert Holleyman and I am President and CEO of the Business Software Alliance (BSA).[1]

BSA represents the world's leading developers of software, hardware and Internet technologies both in the U.S. and internationally. Our mission is to educate computer users on software copyrights and cyber security, advance public policy that fosters innovation and expands trade opportunities, and fight software piracy. We are headquartered in Washington, D.C., and are active in over 65 countries internationally.

It is a pleasure to be with you today to discuss a serious issue of consumer protection: protecting millions of computer users from those who secretly install software on computers in order to obtain information about those users. Such software goes by the name of "spyware." That is clearly the intent of the SPY BLOCK Act (S.2145) introduced by Chairman Burns and Senators Wyden and Boxer. It is also the intent of the Safeguard Against Privacy Invasions Act (H.R. 2929) introduced by Representatives Bono and Towns.

---

[1] The Business Software Alliance (*www.bsa.org*) is the foremost organization dedicated to promoting a safe and online world. The BSA is the voice of the world's software and Internet industry before governments and with consumers in the international market place. Its members represent the fastest growing industry in the world. The BSA members include: Adobe, Apple, Autodesk, Avid, Bentley Systems, Borland, Cisco Systems, CNC Software/Mastercam, HP, IBM, Intel, Internet Security Systems, Intuit, Macromedia, Microsoft, Network Associates, PeopleSoft, RSA Security, SolidWorks, Sybase, Symantec, UGS PLM Solutions Inc. and VERITAS Software.

Mr. Chairman, you and the other members of this Committee have been leaders in adapting our laws to the information age—carefully and deliberately, with a scalpel not a saw. This morning I would like to make three points.

First, computer snooping, or spying on computer users, is a reprehensible practice that invades our privacy. However, the problem is with bad behavior, not bad software tools or products.

Second, for that reason Congress should continue to ban the behavior not the technology. The problem is with abuse, not use, of technology.

Third, we believe the bills as introduced can be improved by focusing more directly on punishing the behavior rather than the means by which it is accomplished. Such an approach enables Congress to avoid having to make very difficult decisions about the design and operation of technology.

Stop E-Spying

We agree with the members of this Committee, other Members of Congress, and the public who rightfully complain about those who hijack computers. There is no policy rationale to justify the actions of those who secretly insert a computer program into someone's PC in order to collect information about that individual or his or her computer habits. It is, pure and simple, an invasion of our privacy. It is wrong and it should be stopped. It is also a national problem and needs a national solution.

Clearly some of these invasions of privacy are intended to, and do, cause economic harm. Someone might be trying to gain insider business information or corporate secrets. Others might be engaged in identity theft—a practice that is estimated to cost American consumers more than $50 billion each year. But electronic snooping is no less invasive if the information is being gathered "only" for marketing or research purposes.

Ban Behavior Not Technology

It is essential that we recognize that the problem comes from bad people, not bad products. The same underlying technology that can enable spyware also may power many legitimate applications that benefit millions of computer users everyday.

Let me put it a different way. We don't ban crowbars because *some* people use them to break into houses. We don't ban cars because *some* people use them to flee from a crime. And last year Congress did not ban telephones because *some* people use them to make unwanted marketing calls. Instead, Congress addressed the offensive behavior and established procedures to control telemarketing.

Mr. Chairman, I feel like I am preaching to the choir. The Commerce Committee has been a leader in applying this principle to developing computer technologies.

Just last year you moved aggressively and appropriately to "CAN–SPAM." That legislation criminalized fraudulent conduct and established clear rules for legitimate business to follow. It made it illegal to access a computer without authorization and use it to send out bulk unsolicited commercial electronic mail or to hide or falsify information about the sender or subject matter of spam. The Act also required the inclusion of a functioning return e-mail address and a prohibition on sending messages to recipients who opt not to receive them. It also addressed more "aggravated violations" such as the use of harvested addresses or the automated creation of multiple electronic mail accounts. But what the bill did not do is to get in the way of the continued development of innovative technological solutions to combat spam and protect consumers.

Mr. Chairman, this committee also successfully applied this principle during the encryption battles of the 1990s. You understood well that it was pointless to try and ban a technology prevalent around the world. Your "PRO–CODE" bill in 1996 prohibited the government from designing and mandating encryption standards and promoted the use of commercial encryption. At the same time, you also agreed with Senator Leahy in his legislation, as well as the House bill introduced by Representatives Goodlatte and Lofgren (the "SAFE" Bill), that it was unlawful to use encryption in the commission of a crime.

Even the Communications Decency Act of 1996 (Title V of the Telecommunications Act of 1996), which among other things sought to address the problem of on-line pornography and minors, did *not* ban the then emerging "interactive computer service." Instead the Act criminalized the use of such a service to send or display obscene and indecent content to those under 18. The Act also established a defense for those who in good faith took reasonable, effective and appropriate actions to restrict or prevent access by minors (including technological means to do so—) but precluded the FCC from endorsing, approving, sanctioning or permitting particular products.

This built on the underlying approach of the 1984 Computer Fraud & Abuse Act which has been amended many times since to expand and strengthen its criminal and civil penalties against computer abusers. This statute penalizes those who access a computer without appropriate authorization and cause broadly defined damage. This statute addresses both those who trespass in cyberspace for commercial gain as well as those who seek to cause harm by launching computer viruses. Indeed, one possible solution to the problem of electronic snooping would be to make illegal the act of commercializing information obtained through surreptitious means.

Why has Congress consistently prohibited conduct not technology? Why has Congress refrained from interfering with the marketplace by dictating the design or operations of computers and consumer electronics?

Congress has wisely avoided technology mandates because you understand that the U.S. technology industry is the envy of the world. It has been responsible for incredible improvements in productivity, millions of jobs, billions of dollars in exports, and immense benefits to every consumer. Government intervention that replaces marketplace solutions with governmental decisions endangers America's technology leadership and hurts users of technology products by stifling innovation, freezing in place particular technologies, impairing product performance, and increasing consumer costs.

Focus and Improve The Legislation

We believe the pending legislation should be changed to focus even more clearly on *what* we are trying to stop, *not* the technology tools to do so. We also think that the most immediate, concrete and compelling problem is electronic *spying*—the unauthorized acquisition and use of information from individuals.

Currently the SPY BLOCK bill has numerous definitions, requirements and exemptions which involve making technical decisions about the operations of today's computers—as well as the direction of future technology. The bill:

- attempts to define computer software, cookie, install; network information; information collection feature, advertising feature, distributed computing feature, and settings modification feature;
- in the case of advertising, distributed computing, and settings modification features requires descriptions of how those features will operate on, and with, a particular computer (*e.g.,* "the nature, volume of information or messages, and the likely impact on the computer's processing capacity of any computational or processing tasks the computer software will cause the computer to perform . . .");
- directs certain technical uninstall operations; and
- necessarily seeks to exempt "any feature of computer software that is reasonably needed to provide capability for general purpose online browsing, electronic mail, or instant messaging . . . determine whether or not the user of computer is licensed or authorized to use the computer software and provide technical support for the use of the computer software by the user of the computer."

We believe the problems inherent in such an approach can be avoided if Congress instead focuses directly on the behavior we are trying to stop: the unauthorized acquisition and commercialization of information.

We suggest that Congress simply prohibit the distribution in interstate commerce of user information obtained electronically from an individual's computer, unless the person seeking to sell the information can show that it was collected with user's explicit permission or that it was obtained from an unaffiliated entity that represents it had collected the information with such permission. Such an approach significantly mitigates the definitional issues in the bill as introduced—and their implications for the development and use of technology—while achieving the objectives of the legislation.

We also believe that what the bill calls advertising, distributed computing, and settings modification features should not be included in this legislation. None of these issues has risen to the same level of concern or been examined nearly as much as electronic spying. Each of these areas also raises separate and distinct substantive and political issues.

For example, having just spent nearly a year implementing legislation to control spam, we are concerned that additional legislation on advertising at this point would detract from the current focus on spying. We also think it is worthwhile to more closely examine existing laws that address deceptive advertising and business practices. Similarly, the case of distributed computing raises new questions. We understand the concern about "zombie" machines utilized without consent—as opposed to the enthusiastic voluntary participation of tens of thousands in the search for ex-

traterrestrial intelligence (the SETI project). But the concept of "grid computing" is just emerging as a serious commercial enterprise and we would be hesitant to casually address it in this bill. Finally, we believe the area of settings as well as their modification is integrally related to on-going efforts to address cybersecurity concerns. Once again, we would be reluctant to address those issues in this bill. As many of the Committee's members know, BSA has been extremely active in efforts to making computing safer and more secure. BSA was one of the hosts and cosponsors of the Department of Homeland Security Cybersecurity Summit last December and throughout this month we are announcing the significant results from private sector efforts initiated at the summit.

More generally, we note that each of these areas may also be amenable to technological and business practices. We think Congress should be careful not to preclude the evolution of tools and marketplace solutions.

With respect to enforcement, we agree that the FTC should be given primary responsibility. The FTC should treat violations as an unfair or deceptive act under the FTC Act. We understand that other regulatory agencies may have enforcement responsibility in other areas.

We also believe that the Department of Justice should be authorized and empowered to subject those who violate the legislation to criminal fees and imprisonment under Title 18 of the United States Code. We should send a clear message that engaging in electronic spying is reprehensible and will not be tolerated.

However, we think that the State Attorneys General should be given enforcement authority in this area only if we have a Federal standard. Remote access electronic spying through "spyware" is a national problem. We think it should be treated as such. The obvious problems with empowering State Attorneys General in the absence of a Federal standard is the prospect for many different enforcement actions based on many different theories and many different standards.

Conclusion

Thank you again for this opportunity to comment on the issue of "spyware" and the SPY BLOCK bill. Working together, I believe the bill can be improved to more directly and effectively address the issue we are all most concerned about: electronic spying.

Senator BURNS. Thank you. We appreciate that very much. Now Jerry Berman, President of the Center for Democracy and Technology, and welcome Mr. Berman.

STATEMENT OF JERRY BERMAN, PRESIDENT, THE CENTER FOR DEMOCRACY & TECHNOLOGY

Mr. BERMAN. Thank you, Senator and Senator Burns, Senator Wyden, again, you are in the forefront of trying to protect privacy and user control of their computers on the Internet and we applaud you, both for your earlier efforts on behalf of trying to pass general privacy legislation, which I think is also involved in this issue, and also to try and craft a bill to deal with this very pernicious problem.

But I want to caution that before we rush to judgment we need Federal intervention here. We don't need a plethora of state statutes, but we really have to spend a little time, take a deep breath, and try and define what we're after here, because if we're overbroad and include all computer software, I think it will be a nightmare to carve out the exceptions of what we're really worried about, and spyware has been defined very broadly. Your bill begins to carve down and deal with the real problems.

But in all of these cases, they may be over inclusive and only talk about privacy when the problem may be broader than that and go beyond privacy to whether, as you point out, consumers can control their own computers and whether they're being hijacked, and that doesn't fit under this, quote, spyware, it's something bigger

than that. And I think we've got to put some of this terminology around and not get confused by it.

I agree with Mr. Holleyman that we need to step back and say, what is the behavior that we're worried about here, what gets us upset about software which performs functions which is being downloaded on your computer when you click on an ad, when you go and get a free service like Kazaa or in a peer-to-peer network or through e-mail or just by browsing on the Internet. Suddenly software is being downloaded on your computer and it is performing certain functions. What is the behavior that's being performed by specific software, not all software but specific software that we care about?

One, I give you three categories. One is software of spyware, if you like, that is collecting information, personal information from you on your site without notice or consent at all and delivering it to another party. That's a clear snoopy privacy violation and it applies to keystroke loggers and a whole bunch of other technologies, but rather than focus on the technology, focus on the behavior.

The second category is information that is being collected about you and delivered to another site or to another person with inadequate notice and consent. They're saying, you consented, you clicked on the site, it popped up an end user licensing agreement six pages long, somewhere in there it said you're consenting to receive ads, you're consenting to give us information, and as part of your Web browsing experience someone clicked on it, maybe your son clicked on it at night, my son clicked on it at night and now a software program is resident in my computer that's collecting information and sending it to another party. I don't think that we need to deal with inadequate notice and consent.

There's a third category which goes beyond spyware and privacy altogether. It goes into user control over computer. If I don't have enough notice and consent and I am now—resident on my computer is a program that's popping up ads, they may not collect information, but if I don't really transparently deal with that company when I click and download that software, and I now have a computer that's serving up ads and I may not know anything about it, someone in my family may have clicked on it, but if I agreed to that, is it popping up and letting every user in that family agree to it?

There's this third category where your computer's being hijacked. They take over your Web browsing experience. We have just filed a complaint at the Federal Trade Commission about a company that you click, you download the software, it opens up your disk drive, it pops up a note and says your computer lacks a lot of security and it advertises on your Web page for spy block and it's Spy Wiper and it's saying you need to buy this software. That is privacy, that's hijacking my computer, and it almost amounts, I think, to computer fraud and abuse under the computer fraud and abuse statute.

Which brings us—all of this behavior—I want to cut my testimony short but say, if we define the behaviors, then we can begin to pick at several different solutions bases. What needs to be covered by general privacy legislation? It would be interesting to only cover spyware when the notice and collection of information un-

fairly applies to websites too and other outliers. Why don't we go back to principle one?

The second issue is we need to look at what—is our Federal Trade Commission complaint going to work? If it is, or the computer fraud and abuse statute applies or ECBA applies, we need to sort that out so we're not duplicating and creating another law.

Beyond that, we need to look at how technology being offered by AOL and Earthlink allows us to sweep spyware. It's a combination again, as in the spam area. We need legislation, we need technology, we need industry practices, but we need to come together and help define that problem. That's why we've written a report, that's why we have a working group, that's why we're here today, that's why we're going to the Federal Trade Commission on April 9.

That's enough for now. I'm anxious to work with all of you to try and resolve this issue. Thank you.

[The prepared statement of Mr. Berman follows:]

PREPARED STATEMENT OF JERRY BERMAN, PRESIDENT,
THE CENTER FOR DEMOCRACY & TECHNOLOGY

Mr. Chairman and members of the Committee, the Center for Democracy & Technology (CDT) is pleased to have this opportunity to speak to you about the growing threat to consumers and Internet users posed by spyware and other invasive or deceptive software applications.

CDT is a non-profit, public interest organization dedicated to preserving and promoting privacy and other democratic values and civil liberties on the Internet. CDT has been deeply engaged in the policy debate about the issues raised by so-called "spyware." In November, 2003, CDT released a report "Ghosts in Our Machines: Background and Policy Proposals on the 'Spyware' Problem,"[1] providing background on the spyware issue, evaluating policy and other solutions, and presenting advice for Internet users about how to protect their personal information and their computers from these programs. At the same time, CDT launched our public "Campaign Against Spyware," calling for Internet users to send us descriptions of the problems they have encountered with these invasive applications.[2] CDT is also engaging in in-depth meetings with the wide range of stakeholders in the spyware issue, including ISPs, software companies, and consumer groups.

The proliferation of invasive software referred to as "spyware" is a large and rapidly growing concern. These deceptive applications compromise users' control over their own computers and Internet connections, and over the collection and sharing of their personal information. We praise the chairman and this Committee for holding this hearing on S. 2145—the SPY BLOCK Act—and thereby bringing public attention to this serious and complex issue.

In our testimony today, we hope to address three principal questions:

- *What is "spyware?"* The term spyware is extremely difficult to define precisely, and can itself be misleading. The term has been used to describe a wide and diverse range of software. What these programs have in common is a lack of transparency and an absence of respect for users' ability to control their own computers and Internet connections.
- *How bad is the problem?* It is difficult to precisely quantify the damage caused by these invasive applications—but it is clear that the problem is severe. Spyware is widespread and can threaten privacy, security, and computer performance. Even the less invasive forms of spyware can seriously inconvenience users and impose serious strains on the technical support resources of schools and legitimate businesses.
- *How can we respond to the problem?* Responding to the problem of spyware requires a multifaceted approach.
  - Existing law could go a long way toward reducing the problem of spyware. While longstanding fraud statutes already cover many of the issues raised by

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

these applications, currently they are rarely enforced against spyware programmers and distributors. We encourage Congress to provide law enforcement with the necessary resources to understand the phenomenon of spyware and to bring to bear strong enforcement of these laws.

- Fundamental to the issue of spyware is the overarching concern about online Internet privacy. Legislation to address the collection and sharing of information on the Internet would resolve many of the privacy issues raised by spyware. We look to Congress to seize this important opportunity to address this larger issue. If we do not deal with the broad Internet privacy concerns now, in the context of spyware, we will undoubtedly find ourselves confronted by them yet again when they are raised anew by some other, as yet unanticipated, technology.
- To be effective, legislation and enforcement approaches will have to be carried out concurrently with better consumer education, industry self-regulation and the development of new anti-spyware technologies.

Legislation directed at some of the specific issues raised by software—such as notice and consent for installation—may also have a role to play. While crafting such legislation will be difficult, the SPY BLOCK Act demonstrates the progress that has already been made in our understanding of the spyware problem. The bill plays a critical role in advancing the inquiry about spyware and developing approaches to addressing the issue.

We address each of these questions in more detail in turn below.

I. Understanding and Defining 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. In some cases, it has even been applied to web cookies or system update utilities designed to provide security patches directly to users. Spyware programs can be installed on users' computers in a variety of ways, and can have widely differing functionalities.

What the growing array of invasive programs have in common is a lack of transparency and an absence of respect for users' ability to control their own computers and Internet connections. The debate over precisely how to define the term spyware (as well as other related terms such as "malware" or "adware") has been contentious, in some cases even leading to legal threats between companies.[3] But this semantic dispute diverts attention from the underlying question: Are consumers offered meaningful notice and choice about the programs installed on their computers and the ways in which their computers and Internet connections are used?

The most egregious forms of spyware (sometimes called "snoopware" to distinguish them from other categories) are typically stand-alone programs installed intentionally by one user onto a computer used by others. Some capture all keystrokes and record periodic screen shots, while others are more focused, collecting lists of websites visited or suspected passwords. These programs have legal uses (*e.g.,* for certain narrow kinds of employee monitoring) as well as many clearly illegal ones.

The more widespread spyware problem is that of applications installed on Internet users' computers in the course of browsing online or downloading other unrelated software. Users are typically unaware that these programs are being installed on their computers. Many "piggyback" on other free applications, such as screen savers, system utilities, or peer-to-peer filesharing programs. In many cases, the only notice to the user about installation of such a secondary program is buried in a long and legalistic "end user licensing agreement." In some instances, no notice of the bundling is provided at all. Other programs trick users into authorizing installations through deceptive browser pop-ups, or exploit security holes to install themselves automatically when a user visits a particular website. In some instances, once a program is installed, it begins to download and install other software with no notice to the end user.

Spyware programs perform a variety of functions once they have gained access to a computer. Many track users' web browsing and deliver pop-up advertisements. While there is nothing inherently objectionable about using advertising, including targeted advertising, as a means to support free software, advertising software must function in a way that is transparent to users, and users must have control over its installation and the ability to remove it.

---

[3] *See, e.g.,* Paul Festa, "See you later, anti-Gators," *CNET.com,* October 22, 2003 (available at: *http://news.com.com/2100-1032_3-5095051.html*)

Other spyware programs can change the appearance of websites, modify users' "start" and "search" pages in their browsers, or change low level system settings without notifying users or obtaining their consent. Some will even co-opt users' Internet connections to send out spam. Such software is often responsible for significant reductions in computer performance and system stability.

Although much of the discussion about the spyware problem to date has focused on the privacy dimension of the issue, clearly many of these behaviors raise concerns beyond privacy. The term spyware itself can be misleading in some of these cases; arguably, a better term would be "trespassware."

Many spyware applications resist uninstallation. For example, advertising programs that are originally installed as part of a "bundle" with other free software may not be removed when the main application is uninstalled. In some cases, spyware applications do not appear in the standard "Add/Remove" programs or other uninstallation feature of the system. In egregious instances, some programs reportedly even reinstall themselves after the user has made deliberate efforts to eliminate them.

No single behavior of this kind defines "spyware." However, together they characterize the transparency and control problems common to such applications. Disagreements will continue about whether particular applications do or not deserve this label. In the end, it may be best to think of spyware not as a discrete and well defined category, but as the bad end of a spectrum of software practices, ranging from industry best practices for transparency, notice, and control on one end, to clearly deceptive and fraudulent behaviors on the other. Unfortunately, the resistance of spyware to easy definition makes writing legislation to address the problem difficult, as we discuss in detail in Section III below.

II. Severity of the Spyware Threat

It is difficult to quantify the spyware problem because of the definitional questions mentioned above, and because the speed with which new spyware applications can appear and change makes reliable detection of the programs difficult. However, several indicators point toward the severity of the problem.

Since CDT launched our public "Campaign Against Spyware" in November 2003, we received over 300 accounts of problems encountered with various spyware applications. The sources of the responses demonstrate that the problem is pervasive—respondents included individuals dealing with the issue on corporate networks, on computers in schools, and on government networks. These users name a wide array of specific programs and identify several categories of concerns, including loss of privacy, decreased stability, and the inability to use their computer, either because of barrages of pop-ups, or as a result of severely diminished performance.

System administrators also responded to our "Campaign Against Spyware." One of the biggest concerns raised by network administrators relates to the security holes created by these applications. Some spyware programs open major vulnerabilities by including the capability to automatically download and install additional pieces of code with minimal security safeguards. This capability is often part of an "auto-update" component.[4]

Network administrators report that spyware is as much or more of a problem than spam, viruses, or other security maintenance. One administrator told us that as many as 90 percent of the computers on the networks he manages have been infected with some variety of "spyware." Another technical support worker reported that the majority of the problems he encounters can be traced back to "spyware," and that his first recommendation to correct stability or performance problems is to run one of the free spyware search and removal utilities available on the Internet.

In our discussions with industry, CDT learned that invasive spyware applications also cause substantial harm to ISPs and distributors of legitimate software. In many cases, consumers are mistakenly led to believe that the problems resulting from spyware applications are a problem with another, more visible application or with their Internet provider. This confusion places a substantial burden on the support departments of providers of those legitimate applications and services. Not only are affected users required to pay for otherwise unnecessary technical support calls, but those calls impose significant costs on businesses offering the support. Some industry representatives we talked to estimated that the additional costs run in the millions or tens of millions of dollars.

---

[4] *See, e.g.,* Saroiu, Stefan, Steven Gribble, and Henry Levy. "Measurement and Analysis of Spyware in a University Environment" *Proceedings of the First Symposium on Networked Systems Design and Implementation,* March 2004 (available at: *http://www.cs.washington.edu/homes/gribble/papers/spyware.pdf*).

III. Responses to Spyware

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

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

Legislation to establish standards for privacy, notice, and consent specifically for software, such as the SPY BLOCK act currently before this Committee, may play an important role as well. The challenge to such efforts is in crafting language that effectively addresses the spyware issue without unnecessarily burdening legitimate software developers or unintentionally hindering innovation. We believe the current bill represents a major step forward, although several concerns still exist.

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

Enforcement of Existing Law

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

Title 5 of the Federal Trade Commission Act is most directly applicable to the most common varieties of spyware. We believe that many of the more invasive forms of spyware discussed above clearly fall under the FTC's jurisdiction over unfair and deceptive trade practices.[5] To our knowledge, the FTC so far has not brought any major actions against spyware makers or spyware distributing companies. In February, CDT filed a complaint with the FTC against two companies for engaging in "browser hijacking" to display deceptive advertisements to consumers for software sold by one of the companies.[6]

The FTC's plans for a workshop in April on "Monitoring Software on Your PC: Spyware, Adware, and Other Software," is an encouraging indication that the Commission is devoting greater attention to this issue. CDT hopes that the clear message emerges from this workshop that the FTC must take a more prominent role in addressing this issue.

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

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

In addition to Federal laws, many states have long-standing fraud statutes that would allow state attorneys general to take action against invasive or deceptive soft-

---

[5] Examples of clearly deceptive or unfair practices include:

- installing unwanted applications without giving users notice in the end user license agreement or another form;
- providing notice only in a license agreement that is misleading or unclear, leading consumers to think they are downloading one program when in fact they are downloading and installing an application that does something completely different;
- utilizing consumer resources such as computer power or bandwidth or that capture personal information without consent; or
- distributing programs that evade uninstallation.

[6] *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*).

ware. Like their Federal counterparts, these laws have not been strongly enforced to date.

New Legislation

CDT has argued that the most effective way to address the spyware problem through legislation is in the context of online privacy generally. Specifically, we believe that the privacy dimension of spyware would best be addressed through baseline Internet privacy legislation that is applicable to online information collection and sharing irrespective of the technology or application. CDT has advocated such legislation before the Senate Commerce Committee and in other fora. Until we address the online privacy concern, new privacy issues will arise as we encounter new online technologies and applications.

At the same time, certain aspects of the spyware problem extend beyond the privacy issues. Privacy legislation would not, for example, apply to software that commandeers computing resources but does not collect or share user information. A comprehensive legislative solution to spyware should address the user-control aspects of the issue—piggybacking, avoiding uninstallation, and so on.

The SPY BLOCK Act currently before this Committee represents an important first step towards addressing some of these problems. We appreciate the desire to craft targeted legislation focusing on some of the specific problems raised by spyware, and CDT applauds Senators Burns, Wyden, and Boxer for bringing attention to these important questions. CDT strongly supports the goal of the SPY BLOCK Act—to assure that users are provided with meaningful notice and choice about the applications that run on their computers.

At the same time, we wish to emphasize the complexity of such efforts. The broad industry opposition to an anti-spyware bill recently passed in the Utah legislature, based on potential unintended consequences of the bill for legitimate software companies, demonstrates the difficulties that can be introduced by such legislation if it is not carefully drafted.[7]

Recognizing that development of appropriate standards for consumer software notice is still in preliminary stages, we suggest two areas of the SPY BLOCK Act that warrant further consideration and may require revision.

- *Standards for Notice*—Providing consumers with informative, accurate notice is a challenging task. Ongoing efforts to craft "short notices" in the context of privacy statements under the Gramm-Leach-Bliley Act both demonstrate the complexity of this problem and may provide a valuable model for the kind of notices that are appropriate in the context of downloadable software. Many so-called "spyware" applications already provide minimal notice to consumers buried in legalistic licensing agreements that come with bundled software. (Programs that do not provide even this level of notice are probably already illegal, as described above.) However, such minimal notice does not provide consumers the opportunity to make meaningful and informed choices. To be effective, legislation will have to address the difficult issue of how best to ensure that the information that accompanies software is appropriately clear, distilled, and contextualized to allow users to make informed decisions. Simply requiring that programs list information prior to installation may not be enough. However, a bill that will burden users by prompting users for choice too often will not be effective either.
- *Scope*—As currently structured, the SPY BLOCK Act covers almost all software, but provides specific exemptions for certain kinds of "general purpose" software and certain specific uses of information. CDT is concerned that this approach creates difficulties for software developers while imposing unrealistic burdens on legislators. This tack requires that legislators develop a comprehensive list of functions for which the requirements of the bill are not appropriate. Creating such a list for existing technologies is challenging in itself. Moreover, such a list will likely become outdated as soon as new technologies are developed, or as the categories defined in the law shift. CDT has argued that privacy laws should be neutral with respect to technologies, and we believe the same principle applies here.

We believe that valuable insight into the questions of scope and appropriate notice for consumer software are likely to emerge from ongoing industry and public interest efforts to define best practices, discussed below, and from the FTC's April Workshop in spyware. We encourage the Committee to incorporate the results of these efforts into refinements of the current bill.

---

[7] *See, e.g.,* Ross Fadner, "Leading Internet Providers Oppose Passage of Spyware Control Act," *MediaPost,* March 15, 2004 (available at: *http://www.mediapost.com/dtls__dsp__news.cfm?newsID=242077*)

Non-Regulatory Approaches

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

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

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

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

The IT industry has initially been slow to undertake such efforts. However, increasing public concern about spyware and the growing burden placed on the providers of legitimate software by these invasive applications has led to more industry attention on this front.[8]

CDT believes Congress can have an immediate positive impact by encouraging industry to continue to develop these efforts toward self regulation.

IV. Conclusion

Users should have control over what programs are installed on their computers and over how their Internet connections are used. They should be able to rely on a predictable web-browsing experience to remove for any reason and at any time programs they don't want. The widespread proliferation of invasive software applications takes away this control.

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

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

Senator BURNS. Thank you, Mr. Berman. Dr. John Levine, thank you for coming today.

STATEMENT OF DR. JOHN LEVINE, PRESIDENT AND CEO, TAUGHANNOCK NETWORKS, AND AUTHOR, THE INTERNET FOR DUMMIES

Dr. LEVINE. Thank you, Mr. Chairman, Senators. I'm John Levine, I'm the president of Taughannock Networks, named after a local waterfall, and I've written a variety of books, including the re-

[8] *See, e.g.,* Earthlink press release: "Earthlink Offers Free Spyware Analysis Tool to All Internet Users," January 14, 2004 (available at: *http://www.earthlink.net/about/press/pr_analysis/*); America Online press release: "America Online Announces Spyware Protection for Members," January 6, 2004 (available at: *http://media.aoltimewarner.com/media/newmedia/cb_press_view.cfm?release_num=55253697).*

cent, *Fighting Spam for Dummies,* which I hope CAN SPAM will soon make obsolete.

Senator BURNS. That's just what I need.

Dr. LEVINE. Well, this one's for you. And I am the Chair or Co-Chair of a variety of grass roots organizations like the—I serve on the board of the Coalition Against Unsolicited Commercial E-mail and I Co-Chair the Anti-Spam Research Group, which is a technical research group.

But you've asked me to come today and talk about spyware, which I'm happy to do, because I happened to read the user mail sent to the Anti-Spam Coalition and every day I get mail from people saying spam is bad, but spyware is worse, how do I get rid of this junk? So although it has not been my primary interest in the past, it's certainly one that's coming up and one that's very interesting for many of the same reasons related to privacy and consumer protection.

I can divide spyware into a variety of sub-areas, which I think I don't need to do, because in the previous comments it's clear that everybody understands what they are. But I would like to back off and echo some of Mr. Berman's comments that computers in everyday life, and the way they work and they way they integrate into people's lives is very new and we don't yet have laws and customs that describe how people react with software and if you have a computer which has some software from the vendor and some software from a website and some software from third parties, how they all react and what the experience for a computer user is.

And it's sort of as though, if somebody came and said, I have a great new business plan, I'm going to open up newspaper boxes and I'm going to stick my own ads in the paper and somebody says, you can't do that. He says, of course I can, I paid 50 cents to get into the box. That kind of argument somewhat reminds me of some of the things I hear about spyware. It's just like, well, you can do it, and down in paragraph 73 of some click-through agreement we said it was OK.

I mean, to me, I see two issues. The first is an issue of consumer protection. With the adware that pops up ads and replaces ads in websites, consumers are completely confused. They don't know where the ads are coming from. All they know is they don't like them and they dislike ads that are popped up by websites that actually place them, they dislike ads that are popped up by software like WhenU's, they feel like they're totally out of control and they don't know whom to blame. So in that case there's a real issue of consumer confusion. I think it's a consumer protection issue.

Beyond that, spyware presents a privacy problem because people click and say, yes, you can install your program and then it collects vast amounts of information very indiscriminately, and I have a bunch of scenarios in my written testimony. For example, if you are applying for a bank account online and a piece of spyware scrapes the data from that application and sends it off to the spyware vendor, the spyware vendor now knows enough about you to commit identify theft. Or if you are conferring with a close relative or with your doctor or with your lawyer, they can collect information to do anything from sending you bogus ads saying, oh forget that chemotherapy for your tumor, we have apricot seeds, to blackmail.

These are enormous privacy issues and I think that we really need to step back and look at them as an overall issue of consumers and computers, and although the spyware issue is important, I think it's just one step on the way to coming up with sort of a general privacy and consumer protection policy that will affect all the ways that vendors and consumers and computers interrelate.

I have some comments on the individual bill. It's a very well-crafted bill dealing with the specific issue of notice of spyware. I have two concerns. First is that I am concerned how realistic it is to expect people to understand the notice they're given and to click through, particularly when you have computers that are used by adults and by children, particularly when frequently the notice is down in page after page of boring boilerplate.

And I would encourage you to consider allowing consumers to create a spy-free zone, just the way the Do Not Call list and the possible Do Not Spam list will allow people to put on notice once saying, we don't want this particular kind of violation here, rather than having to negotiate each time a vendor comes in and says I want to do this.

My other concern is with enforcement. The Do Not Call list is very effective because the enforcement ranges from the FCC down through the attorney generals down through individual suits, and I think that this broad range of enforcement is really very effective in making Do Not Call effective, and I would encourage you to consider a similar provision for this bill. Thank you.

[The prepared statement of Dr. Levine follows:]

PREPARED STATEMENT OF DR. JOHN R. LEVINE, PRESIDENT AND CEO, TAUGHANNOCK NETWORKS, AND AUTHOR, THE INTERNET FOR DUMMIES

It is my honor and privilege to submit these comments to the Subcommittee on Communications of the Senate Committee on Commerce, Science, and Transportation for consideration during their hearing on S. 2145, the SPY BLOCK Act.

I am a consultant and author specializing in consumer-oriented Internet topics. I am the primary author of *The Internet for Dummies,* the world's best selling book on the Internet, which has sold over seven million copies in nine editions in over two dozen languages since 1993. I am also the co-author of numerous other books including the recent *Internet Privacy for Dummies* (2002) and *Fighting Spam for Dummies* (2004). In these books, my co-authors and I educate readers regarding online marketing and advertising practices that threaten the privacy of their personal information and/or present the risk of unauthorized collection, use, and abuse, of information about their online activities.

I co-chair the Anti-Spam Research Group (ASRG) of the Internet Research Task Force under the oversight of the Internet Activities Board of the Internet Society. The ASRG is a coordinating forum to coordinate research into and development of technical measures to deal with unwanted e-mail, with broad participation of industry, academia, and independent researchers. I serve on the board of the Coalition Against Unsolicited Commercial E-mail (CAUCE), the leading grass roots anti-spam advocacy organization.

I have spoken at many professional, trade, and government fora such as the 2003 Federal Trade Commission Spam Forum and the upcoming *Enterprise Messaging Decisions* conference in Chicago, May 4–6, 2004, and the *E-mail Technology Conference* in San Francisco, June 16–18, 2004.

I serve on advisory boards related to consumer Internet issues at companies ranging from Orbitz, one of the big three online travel agencies based in Chicago, to Habeas, a small anti-spam certification startup in Palo Alto, CA.

What is Spyware?

Spyware is a general term used to describe software that runs on consumers' personal computers and performs actions that the consumer considers undesirable or

hostile. The term has been applied to a wide variety of different applications, ranging from the arguably legitimate to the egregiously fraudulent. The three most common types of spyware are the following:

- *Adware* monitors the pages fetched by a user's Web browser or other material on the consumer's computer and when it sees particular pages or terms, displays other pages containing advertisements paid for by the spyware's sponsors. So called "Browser Helper Objects" install themselves as part of the Internet Explorer web browser and change the way it works. The changes can be as simple as switching to a different home page, or as complex as redirecting web searches to the spyware vendor's search system rather than the consumer's desired system, or adding new "click here" buttons that lead to sponsors' advertisements.

  In some cases, the adware rewrites the web pages displayed by the browser, substituting ads from adware vendor for the ads originally in the page. This technique has been likened to opening newspaper boxes and pasting one's own ads on top of the ads in the papers.
- *Key loggers* record every key pressed by the computer's user and send the stream of keystrokes back to the spyware's author. More generally, "Activity Monitors" can log and report on any type of consumers' computer usage, such as e-mail send and received, web pages visited, and instant messages exchanged. The data can be used for anything from consumer preference statistics to identity theft.
- *Trojan Horses* allow the spyware author or vendor to remotely control the consumer's computer for the author's purposes. At the point, the most common purpose is probably to send spam.

Although these are the most common current varieties of spyware, variations on these themes and new and different spyware programs are released frequently. We can expect different varieties of spyware to appear in the future.

How Is Spyware Installed on Consumers' PCs?

Spyware distribution is made possible by a combination of the weak security of Microsoft Windows and the inability of consumers to understand the many security-related warnings that their computers currently present to them.

MS Windows generally makes it very easy to install software remotely onto a consumer's PC. While this facility is useful in a corporate environment where an IT department manages computers all over the company, hostile parties can also use it to install spyware without the consumer understanding what's happening. In some cases, whenever a consumer visits a spyware vendor's web page, programming in the web page automatically installs the spyware. In other cases the spyware is installed as part of a program that performs a desirable function unrelated to the spyware features.

Sometimes, the consumer is presented with a warning screen asking whether to install the new program. The warning screen is nearly identical to the warning screens that appear when a web page needs a benign application such as one to display "flash" animations. Consumers see such warnings so often, and have so little information with which to evaluate any particular installation request, that they rarely reject an installation request. In many other cases, security weaknesses in Windows make it possible to install spyware without the consumer's knowledge or consent.

Some computer manufacturers are now shipping PCs with spyware pre-installed. This means that users will have to go to extra time and expense to remove the spyware from their new computers to bring it to a normal usable state.

Is All Software that Communicates with Remote Computers Spyware?

No. In some cases, consumers deliberately install software with remote communication features to participate in a large-scale computing project or a multi-player game or other activity. For example, many of my computers run a program from the volunteer-run distributed.net that solves large mathematical and cryptographic problems. Another well-known project called Seti@Home, coordinated at the University of California at Berkeley, uses consumers' computers to analyze data from radio telescopes, looking for evidence of intelligent signals from outer space. In both of these cases, the consumer runs the program because he or she actively wants to participate in the projects, the programs make no changes to the computer's configuration (other than an optional screen saver with Seti@Home) and the programs return no data about the consumer other than an optional e-mail address or "handle" if he or she wants to be counted in the statistics that the projects publish.

Another common situation is straightforward advertisement supported software. For example, the popular Eudora e-mail program and Opera web browser are distributed in free versions that display small advertisements in clearly labelled windows within the application. The ads do not interfere with the normal operation of the program. The consumer is clearly informed that if he or she purchases a paid registration for the program, the ads will go away.

Any legislation related to spyware should be crafted so as not to interfere with legitimate applications such as these.

How Do Consumers Feel about Spyware?

They hate it. Although spyware has never been my primary area of activity, in my role as online postmaster for CAUCE, I get mail almost daily from consumers complaining about spyware and asking what they can do about it. On the *Internet Privacy for Dummies* website at *http://www.privacyfordummies.com,* a page about dealing with spyware is the most frequently visited on the entire site.

A small anti-spyware industry has arisen with programs like Adaware, from *http://www.lavasoftusa.com,* and Spybot Search and Destroy, from *http://www.safer-networking.org,* that detect and remove spyware from consumers' computers. Companies now routinely recommend that their employees install and use one of these programs on a regular basis to clean off any spyware that may have installed itself.

Spyware is frequently written so as to be difficult or impossible to remove from consumers' computers. It rarely comes with an uninstall program, as is standard with other PC software, or it comes with an uninstaller that doesn't actually remove the spyware. Some of the more egregious spyware attempts to delete anti-spyware programs such as Adaware and Spybot from computers, and to reconfigure web browsers to make it impossible to reach anti-spyware websites or to install anti-spyware software from those sites.

Consumers clearly perceive spyware as an illegitimate use of their computers, and spyware is rarely if ever installed with the informed consent of the computer's owner.

What Policy Problems Does Spyware Present?

Spyware presents two separate policy issues, consumer protection and privacy.

The consumer protection issue is that consumers don't provide consent when spyware is installed on their computers, they don't understand what the spyware on their computer is doing, and when they become aware of its presence, they invariably want to get rid of it. In principle, this issue could be addressed by better disclosure at the time the spyware is downloaded, installed, or activated. But in practice, I am skeptical that disclosure would be effective. The behavior of spyware is often quite complex, and a disclosure of that behavior equally complex, to the point that many consumers would see the disclosure but wouldn't understand its implications and would be unable to make an informed decision whether to accept it or not.

Furthermore, adware that shows its own advertisements in connection with web pages that a computer's user has requested causes severe consumer confusion. The consumer cannot easily tell what ads are part of the web page, and what ads may have been added or replaced by the spyware. Consumers incorrectly assume that advertisements are provided or endorsed by the author of the web page, rather than by the spyware vendor. If the advertisements are inappropriate or offensive, the consumer blames the web page author, rather than the spyware vendor that actually provided the advertisements. In some cases, the advertisements inserted by adware are for sexually oriented materials, although the spyware vendor has no way of knowing the age of the computer's user.

I am aware of at least one group of lawsuits filed by mainstream advertisers against Claria, formerly Gator, a vendor of adware that is typically installed with peer-to-peer applications such as Kazaa, due to its advertisement insertion practices.

The privacy issue is that spyware often collects personal information about the users of computers on which it is installed. This is an issue for any computer user, and is doubly so for users under the age of 13 who can't consent to collection of information about themselves.

One could argue that in principle this problem could also be addressed by better disclosure, but I believe there are public policy reasons that it's not a good idea to let people sell their privacy rights. The law has long forbidden certain kinds of consumer transactions (selling parts of one's own body, for example) as contrary to the public interest, even if the consumer wishes to enter into such a transaction voluntarily and with full notice. I believe that there are sound reasons to treat the sale

of one's privacy as contrary to public policy. The value of one's privacy is great, and the amounts offered in exchange for it are rarely large. Once one's privacy is traded away, it is difficult or impossible to regain, and the implications of giving it up are frequently far greater than what a consumer would foresee.

Since spyware can and often does collect information about all of a computer user's activities on the computer, and software cannot tell private from non-private information on a computer, the opportunities for abuse are vast. For example, consumers often apply for mortgages, bank accounts, brokerage accounts, and other financial accounts online. If spyware sends the information from one of these applications back to the spyware vendor, the vendor has everything necessary to commit identity theft. Consumers often use e-mail or instant messages to communicate privately with friends and relatives, or with trusted personal advisors such as lawyers, accountants, and doctors. If spyware collects the contents of those messages, which is technically easy to do, the possibilities for abuse range from medical fraud ("our apricot seeds will cure your cancer better than old fashioned chemotherapy") to blackmail.

Many consumers underestimate the damage from privacy invasions on the assumption that if they conduct their lives in a legal and ethical fashion, they have nothing to hide. The reality is that some areas of everyone's life are private, and the damage from invading those private areas is real, substantial, and very difficult to cure.

S.2145 as currently written is a well-crafted attempt to deal with spyware problems by mandating disclosure and minimal good software practices. I have two reservations about the bill in its current form.

The first is that I am not confident that disclosure is the most effective way to deal with spyware problems. In view of the universal distaste of consumers for spyware, and their invariable desire to get rid of it when they find it installed on their computers, it would make far more sense to ban spyware outright, or to provide a simple way, analogous to the telemarketer do-not-call system, that a consumer could provide one-time permanent notice that spyware is unwelcome on his or her computer, rather than having to wade through notices and disclosures every time a spyware vendor wants to sneak something onto the consumer's PC.

My other concern is for enforcement. The current draft leaves enforcement primarily to the FTC and to state Attorneys General without providing any new funding for enforcement. In view of the large number of spyware authors and vendors, and the budget pressures on all enforcement agencies, it seems unlikely that they will be able to take action against any but the largest violators. One of the reasons that the existing do-not-call system is so effective against telemarketers is that the law specifies statutory damages for consumers who are the victims of illegal telemarketing calls, and allows consumers who are sufficiently motivated to sue for modest but meaningful amounts. A similar provision to let consumers recover for spyware violations would make an anti-spyware law far more effective without requiring new funding for the FTC or other agencies.

Senator BURNS. Thank you. We've been joined by Senator Allen of Virginia, who chairs our high-tech conference and does a great job at that and, of course, represents a great technology community here in Northern Virginia. Thank you, Senator Allen. Do you want to make a statement or ask a question or do you want to play football?

STATEMENT OF HON. GEORGE ALLEN,
U.S. SENATOR FROM VIRGINIA

Senator ALLEN. I'd rather play football but I didn't bring the ball. It's back in my office. I want to thank you, Mr. Chairman and Senator Wyden for bringing this issue to attention. I was listening to Mr. Berman's nightmare scenario, and I said, God, I was telling my staff, I said, that's what was happening on our computers. It was not just the spyware, it's the pop-ups and things shooting out of the side of it and all the rest and you put it back in, restart it, it all comes through again and it's just—this is broadband that we're all trying to get deployed and so forth, and I'm thinking, God, dial-up was better than this.

Finally, we got someone in there who could install the right technologies to stop it and now being on the Internet and reading articles and so forth is a pleasure without all that interference of pop-up ads and notices that you're being monitored and all the rest.

And when you get to this issue of spyware; I was hearing several of the gentlemen talking about the definition. I think your definition is one that makes pretty much common sense, like a lot of the things you do, Senator, which is very rare around here having some common sense. But it seems to me it would be a software that monitors a computer user's activities, it collects personal information, and shares it without the user's or the consumer's knowledge or their consent.

I look at this from a perspective of a privacy issue, because what you are doing is an invasion of an individual's privacy. I approach this whole debate on what we ought to do similar to the way we handle the online privacy debate in this committee last year.

There's a few points I want to make. Number one, I think that all of us ought to be able to agree as a matter of principle that under no circumstances is it acceptable for someone to secretly or deceptively monitor a consumer's activities online without that consumer's knowledge or consent, and any sort of misleading or false practices associated with spyware, in my view it threatens consumer confidence, I think it ruins, it harms the Internet's viable and usefulness, whether it's for commerce or for access to information. And in that regard, Senator Burns and Senator Wyden, I thank you for identifying this problem with your measure.

Now second, as we examine this legislation and how to handle it, I think we ought to consider all the different options. Like online privacy, I think it's important that we empower individual consumers to make sure they have the information necessary to make reasonable decisions and choices. I think we ought to encourage to the greatest extent possible market-driven solutions to this, and this has been a committee that doesn't like to always dictate the technologies because we like to see the advances in technologies.

Third, as you go through all of these, and listening to the concerns we do have existing laws. You're talking about identify theft. That is currently, presently a crime. We ought to find out how we—maybe those laws need to be made better, but the question of privacy is governed by law, identity theft, fraud, deceptive marketing practices, all are part of the law.

Now, it may be that we have to find a way in the midst of this legislation as we discuss it to make those more enforceable, but those basic principles are there, and just because it's spyware or adware or whatever it may be, it doesn't mean that they're immune from those laws. And so with the technological advances that have grown, I think we ought to be looking at those approaches, enforce the laws we have. I think it's in the interests of the broad technology or Internet community to get this done, to make sure that you don't have people frustrated, aggravated, or sometimes insulted with some of the spyware and the adware with some of the pop-ups that come up that are inappropriate, and we all know what I'm talking about here.

So I'd like to see a market-driven approach or solution. I want us to find ways to enforce our current laws and I do want to work

with you as I have, both of you, great leaders in technology. What we all did with spam, what we've been able to do with Internet privacy matters, I think those would be the guidelines and philosophy I'd like to follow, and thank you again, Mr. Chairman and Senator Wyden for your sterling leadership once again.

Senator BURNS. Thank you, Senator Allen. I have just a couple of questions. Every time we start in on this kind of legislation, and I think Senator Wyden would concur that we spend a lot of time working on definitions, people define different terms and words differently. And we tried to do that in this, and especially it's very important whenever you start talking about this business of privacy. It's a very personal thing.

Now, given what's been happening with the software that's downloaded into your computer that has basically set your computer to be a tool of somebody else and not always of your own, and we know that probably out of the millions of users of computers, probably less than a third of them read *PC Magazine.* What tool do we use to make people aware of this problem? And I'll let anybody comment on that.

Mr. BERMAN. Well, certainly we have to let people know about the problem, and I think that hearings like this and the press coverage and so forth, but I think it's consumer education down at the, at the basic level. Last year and over the last couple of years, industry and public interest organizations like CDT created the Get Net Wise site, which provides information on privacy and what consumers can do about, even about spyware. It's just a beginning, but it's a consumer education program.

But I don't think that we can begin there. We have to give people and the consumers some clear definitions of what we're talking about, and I think that some of the tools that are in your legislation are going to be necessary. It is one thing to find spyware or adware or a software program that takes over your computer and you can't uninstall it, and I don't know any consumer education program outside of a technical manual that's going to help you do that, and you got a technical person.

Not everyone has a Web master like I do to take spyware off of my computer, so we need to, as in CAN SPAM, to provide some requirements. That if software is installed on your computer that it has to be, even with your consent, that it has to be removable, and SPY BLOCK moves in that direction. That's one of the things that no notice bill and no FTC proceeding is going to solve. It is going to require some legislative action.

Senator BURNS. Mr. Holleyman?

Mr. HOLLEYMAN. Mr. Chairman, a couple of things. One, I do think that raising public awareness about this is critical. It's like this hearing, things that have been held in the House, the FTC workshop next month, the publicity on this I think is very important.

Second, I think there will be more tools that will be made available by software developers that will be easily deployed that will let people track this. Third, I think we need aggressive enforcement, and we don't need to wait until a new law is passed, and a new law may be needed. But what we need is aggressive enforce-

ment of existing laws to try to dry up the practice of commercialization of information that's seized in this fashion.

Then I think there are other steps such as industry best practices, working with sort of new upgrades of software that will all yield hopefully to a much better environment than the status quo.

Senator BURNS. Mr. Naider?

Mr. NAIDER. Yes, I'd like to follow up specifically what Mr. Holleyman said in the sense that industry standard-setting is really one of the major opportunities that the SPY BLOCK legislation presents in the sense that one of the themes that you hear emerging from this panel is the notion of consumer control.

Dr. Levine made an interesting point, which is that whether its spyware or adware, a lot of consumers will say they don't like it, and I will readily confess that even WhenU software, we get many consumers who say they don't like it. We've done tens of millions of installs, but many consumers choose to remove it.

The point is, that if you give consumers control and you set a standard by which a consumer makes a choice to install when they have this type of software, particularly adware that shows them ads, each ad is very conspicuously branded and addressed and makes it clear where it's coming from, the user is then easily able to uninstall.

What you then do is you create a standard by which you don't undermine the technology, you don't take the 25 percent of the market that benefits from the technology, but you allow a set of standards to be set that the consumers ultimately do control, and that's ultimately what really infuriates consumers, when they don't have control, when they don't know what's happening to their computer, and when they can't do anything about it, and we do have the opportunity right here to address that.

Senator BURNS. Mr. Levine?

Dr. LEVINE. If I may digress slightly, on the plane down I was reading a funny article about a fellow talking about the 1930s and 1940s appliances in his house. He was talking about a toaster or something, and he said that he learned the hard way that the control on the toaster had a little rubber knob on the end which you had to hold, because if you touched any other part of the toaster, you'd be electrocuted. And we don't build toasters that way anymore, and no doubt at the time the toaster was built, there was a sign saying, only touch the knob.

And I think a certain amount of labeling is useful, but I think that if you have a practice that consumers find so noxious and so uniformly contrary to what they expect, it's like with my example of the newspaper boxes. We could have a campaign to put signs on the boxes saying, danger, don't read newspapers with other people's stickers on them, but I think what we really need is a consistent policy about what sort of data collection is appropriate for computer software and what isn't so that users don't have to be worried every time they click somebody might steal their data, that they can be confident that their computers will work in a way they think is reasonable.

Senator BURNS. Well, I get the feeling that I'm going to have a follow up question for Mr. Holleyman, but I first want to get to my

colleagues and we'll probably have a couple of rounds of questions here, but Senator Wyden.

Senator WYDEN. Mr. Chairman, gentlemen, the first question I'd like to start off with is whether or not you all feel there are legitimate reasons for software that doesn't allow a computer owner to delete it. Let's go right down to it. Maybe some technical reasons and that's what I'm interested in, but I mean, as a general rule it seems to me if the computer owner can choose to install it, he or she ought to be free to uninstall it, but I'd like to see if we can kind of just go right down the row and see if as a general proposition you all share that view. Start with you, Mr. Naider.

Mr. NAIDER. We completely agree with that. Computer owners should have the right to install software and uninstall software. Occasionally, as in our business, for example, you see instances in where a consumer downloads a free piece of software, and in addition to that free piece of software, there's another piece of software that supports the free piece of software, for example, providing coupons and advertising. In those cases, we think the consumer should have the choice to uninstall as well by uninstalling the free piece of software and that goes with it.

But under no circumstances can we imagine a scenario where a computer user shouldn't ultimately be the one to control what is and what is not on their computer.

Senator WYDEN. Anybody on the panel disagree with that? We can just go right down the row and save some time. I just want to see if as a general rule you feel that that's appropriate.

Mr. HOLLEYMAN. I agree with your general rule, with your caveat that there may be technical reasons at times where you cannot uninstall something without harming the operating system, for example.

Senator WYDEN. Jerry?

Mr. BERMAN. I agree that you ought to be able to uninstall and the principle—the right to uninstall, but right now you don't have the right to uninstall a lot of spyware.

Senator WYDEN. Right. Dr. Levine?

Dr. LEVINE. As a general principle, I agree with everybody else. You need to be able to uninstall stuff. But I think what consumers are more interested in is the possibility of breaking stuff apart. For example, they'll install a program that does some useful thing and then it's bundled in with something else that they consider to be spyware, and they consider the program to be useful and the spyware to be useless and they'd like to be able to get rid of one without the other. That's where I think you run into these issues of what's uninstallable and what's not.

Senator WYDEN. I put into the record something that struck me as very plausible in one of the *New York Times* pieces calling for something similar to what we've introduced. They start—and I'll quote here—a good start would be to require all such programs to announce themselves clearly and define their functions, allowing the users to reject software that strikes them as intrusive. Anybody disagree with that?

Mr. BERMAN. The issue is, what software under the, say, for example, legislative rule would have to announce itself and then you get to decide what is intrusive?

Senator WYDEN. Covert, secret.

Mr. BERMAN. Well, if we define it that way, but some of the legislation unintentionally or even intentionally has defined the computer software to include any software resident on your computer and then you get to software that does some monitoring functions, diagnostics and so on, can be covered. It's not defined clearly in terms of computer software that does something that we would consider bad behavior.

Mr. NAIDER. If I could follow up Mr. Berman's comment, I think one of the concerns with the legislation as currently worded is exactly what Mr. Berman is saying, which is that it doesn't say this explicitly in the legislation, but at least with regards to the advertising copy in the legislation, it's implicit that's it talking about pop-up advertising, just some of the language that's used to say it has to have a notice and each ad has to have a link to an uninstall.

When you think about the future of this type of technology, many in the industry believe that software on your desktop, legitimate advertising software, will be done in many, many different ways. It may be in the form of toolbars that are on your computer, it may be embedded within your browser, it maybe is part of the interface of your ISP so that this notion of every piece of software announcing itself in the same way that would be contemplated for something, for example, that does pop-ups may be inappropriate.

And one of the things that we think needs to be studied and looked at in detail with regards to any legislation is not what is the current practice of adware or software-based advertising, but what is the potential future universe of different activities that could take place that are very, very legitimate, very empowering to consumers. Can this bill broadly worded actually hinder that, and that's I think one of the concerns we have with the bill.

Senator WYDEN. Those are legitimate points. What we're trying to do is get at the secrecy, the secrecy that really invades the rights of the consumer that we've all been talking about.

The third area I wanted to ask you about, Dr. Levine, was drive-by downloads and how easy it is to set them up. It strikes me as pretty good target, pretty fertile area for shady kind of people, but why don't you tell us about that?

Dr. LEVINE. It's extremely easy, and it's easy for two reasons. One is that Microsoft Windows, which everybody uses, is just designed in a way that makes it really easy for third parties to install software into it, and in many cases that's fine. If you have a corporate network, the ability of the IT department to maintain all the computers in the company is fine.

And if you have a website that uses a particular kind of audio or animation or something, the ability to say, oops, you need the Flash Player, would you like me to install it for you so you can see this cartoon, that's fine too.

The problem is that the technical line between the Flash Player, which just shows you pretty pictures, and spyware that does malevolent things, is very narrow. It is both easy for people to install stuff without notice, and the other problem is that people install stuff so often, 3 hours it pops up and says, oh, here's a little component we'd like to give you. And from the consumer's point of view, it's very difficult to tell the notice between something malicious.

Senator WYDEN. Just a couple of other quick questions. I know my colleagues want to get into it. Mr. Holleyman, gentlemen, came out for going after electronic spying, but essentially felt that adware wasn't a major concern right now. He said it hadn't risen to the same level of concern. Mr. Berman and Dr. Levine, do you two view the proposition that pop-up ad software isn't yet a key consumer concern?

Mr. BERMAN. I think because there are companies that are providing these programs and without clear notice and consent to the consumer or to all the users of a particular community, I mentioned the family example, that the pop-up ads are becoming in a consumer's mind another form of pop-up spam. In fact some of these programs also allow you to serve spam, but it's the pop-up ads are, I think, a nuisance to computers and interfering. If they don't have consent they are being served content which they really don't want.

Now, the difference between what they want and whether they've consented is really how explicit the notice is, how clear it is, and how simple we make it, and there are no standards for that right now.

Senator WYDEN. Dr. Levine, you?

Dr. LEVINE. There's no question that people hate pop-ups. I consult for one of the large travel websites that's used what we could call "legitimate pop-ups" extensively in their advertising, and they're legitimate in the sense that if you go to a site like ESPN, a site, the pop-ups ads that pop up are actually placed by ESPN and support the website, and even though they're, you know, by any business standard they're legal, people hate them, you know.

And then we go on to the kinds of third party ads where, ads that—advertisements that weren't part of the original website, people hate those even more because they don't know who to blame. So I'd say from the point of view of consumers, it is a very big issue, and it's one that they really would like to have somebody fix.

Senator WYDEN. Yes, I don't want to jump on you on this point, Mr. Holleyman. I know you're sincere on it. But I think if you were to go out across the land today and ask people about pop-up ads software, they'd say, that stuff drives me nuts, I'm outraged by it. And we want to work with you, I mean, you're raising a lot of practical concerns about how to do it. But I got to tell you that we're not jumping you here today.

Mr. HOLLEYMAN. Sir, I think there are two things here. One is we were trying to focus on what we think is the biggest current problem where we can both start deploying current laws and then fill in gaps with new legislation. Second, there's a pending bill before the Utah Governor that she has until, I think, midnight tonight to decide whether to sing or veto, there was a spyware bill passed by the Utah state legislature.

Senator WYDEN. I understand.

Mr. HOLLEYMAN. There was a very broad group of technology companies and associations who met with the Governor last week to urge her to veto that bill to give their legislature another chance to look at this when they come back in session next year.

One of the comments she made, that was made in the letter, and I do not represent advertisers per se, but I will simply pass this

along, was talking about pop-up ads and talking about the importance of enabling local advertisers in Utah to be able to properly tailor advertisements to Utah-based citizens rather than only allowing broad-based national advertisers to have that broad reach.

I don't know what the answer to that is, but I would encourage you to look at the letter that we submitted to the Utah Governor as one of the issues associated with this.

Senator WYDEN. One last question if I might. You, Mr. Holleyman, said that state AGs ought to be given enforcement authority in the area only if we have what you call, you quote, a "Federal standard." So obviously what we think we're doing in the bill is establishing a Federal standard, and what I was curious about was whether this was really something that you want to just deal with as a preemption issue. Are you all calling for preemption? Is that something you'd support, Federal standard preempts states?

Mr. HOLLEYMAN. If Congress moves in this area and determines if legislation is needed to close existing gaps, then there should be a Federal single standard that preempts inconsistent state laws.

Senator WYDEN. Mr. Chairman, thank you.

Senator BURNS. Senator Boxer.

Senator BOXER. As a pop-up ad victim, those things are really the worst, and it's the whole point, I mean, and it shocks you. It's a very disconcerting deal, because when I'm working on my computer I'm working on something, and it's just like, I mean, my grandson knows don't bother Grandma right now. I'd rather be disturbed by him than these idiotic things, some of which are foul.

But here's the point. I think if we do work together and we can make this happen right, you'll wind up being happy because you don't want Utah doing their thing and you don't want California doing their thing and so on and so on and Virginia. We've got to get together here and have some answer to this thing.

Mr. Holleyman, when you say you don't represent advertisers per se, what does that exactly mean?

Mr. HOLLEYMAN. I represent companies who certainly advertise, as most commercial businesses do, but I'm not speaking on the adware issues or representing companies who are making a profit out of selling advertising.

Senator BOXER. Say that—you represent advertisers, but——

Mr. HOLLEYMAN. I represent major companies who all advertise their products, but I'm not representing companies such as the colleague at my right, who are in the business of providing advertising services.

Senator BOXER. OK. Well, you know, I don't want to prolong this because I just, for me certain issues are a no-brainer. This—for what—it's simple. You know, this is not a good thing that's happening to folks, and in the end it's going to drive people away from their computers and that's not a good thing. I am very much in favor of all of this information-gathering, and I can tell you, you're sitting there, you're trying to do some work, you're trying to get information, and you're just bombarded and it all happened because somebody spied on what you were looking and I looked at shoes and they're advertising shoes. This thing has got to go. This is not a good thing. And so, yes, Mr. Berman, I don't have——

Mr. BERMAN. I have problems with pop-up ads from downloaded spyware. I actually have an ad program that runs on my mail program, it's serving me ads, and the reason I'm getting the free mail service is they're serving me ads, they're getting some revenue from it.

I consented to it. It's very clear on my desktop what's happening and if I don't want it I can pay for a different program and the ads disappear. And if I want to uninstall it, I just take that program and get another program. That kind of transparency I think is where consumers want to go.

Also, while we may not like pop-up ads, that is a much larger and different, and sometimes different issue than spyware. Pop-up ads are being served without spyware, and so we got to put things in boxes and say what is the most important thing that we want to deal with.

And I got to one more time make this point, that the privacy issue, which is only one part of this spyware problem, is the collection of information without your consent. It may be through a program on your—but it goes back to Senator Allen, the privacy bill that passed out of the Commerce Committee, it may need—maybe there wasn't a giant Congressional consensus, is still not law. We do not have online privacy legislation which defines the fair information practice for online privacy for websites, for companies doing business on the Internet.

We are relying on important self-regulation. Good companies are doing a great job at trying to give you privacy notices on their website. But I point out when you're dealing with spyware, you're finding out that there are always outlaws and outliers using new technology to do the same thing, take information without notice and consent. And until we have some rules about that, which goes back to Burns/Wyden 1, we're not going to solve the privacy problem, and to try and do it for spyware, like say, well, we have a cookies bill and a spyware bill and a spam bill, it begins to become a crazy quilt, which is what we want to try to avoid when we ask for Federal legislation, some coherent, overall policy.

And we need privacy policy in this area. It doesn't have to be, you know, terribly burdensome, but it has to inform both good companies and bad companies what the rules are here for collecting information about consumers and users on the Internet. We don't have that.

Senator BOXER. Mr. Berman, let me just say, I have no disagreement with anything you said, but I'm also a practical legislator.

Mr. BERMAN. Right.

Senator BOXER. And I can tell you now, the reason I was so proud of my colleagues and teamed up with them on spam and these other issues is because sometimes you can't get that overall, but I agree with you, it's all a matter of consent, that's really the bottom line. But also consent that's obvious, that is easy to figure out, so that it's not such a difficult hurdle that you have to do 17 things to get out of this deal. That isn't any good. It's got to be something straightforward. That's what we've been trying to do.

Mr. BERMAN. This may be one time when consumers are going to become so outraged by this kind of behavior that different laws are going to pass in Utah, pass like that, may not be signed into

law, that it may be the better part of valor to revisit, maybe not in an election year but maybe early next year, trying to develop some baseline standards again as part of the tradeoff of resolving a set of issues that surround, that beg for a solution, but do not beg for a solution that is technology-specific, because that is anathema to innovation and to the Internet to go technology by technology.

Mr. NAIDER. If I can add, specifically for Senator Boxer's very good point about consumers hating pop-ups. I think one of the things that we have to all recognize is that these types of bills are strangely affected by consumers' general dislike for pop-up advertising. For example, if you said to an average consumer, do you like pop-ups, most consumers would say no, I dislike pop-ups. If you said to a consumer, would you want a piece of software that alerts you to a $30-off coupon when you're about to make a purchase, most consumers would say yes.

The important thing is to recognize that the pop-up problem is a much, much, much larger problem online than sort of a narrow problem as a result of either spyware or adware, et cetera, and that in the course of trying to address consumers' concerns with pop-ups, specifically a sense of feeling bombarded or being hit with pop-ups that don't come from anywhere, we have to be very careful about not affecting or ruling out software that can actually be tremendously beneficial.

And when you think about where the Internet is in 5 or 7 years, is it desirable for most computers to have software on their machines that, as a consumer's navigating the Web, in some way, shape, or form is alerting them to maybe three other places where they can buy a mortgage or to a great deal on travel? When you're looking at a hotel in New York City, should a piece of software be allowed to tell you about a place where you can get that hotel for 50 percent off? Many people would say yes, and we just want to make sure that this legislation covers that.

Mr. BERMAN. But there's a problem. It's when, who's saying yes and consenting to this software being loaded on your computer? Many of these pop-up adware programs are added as piggy-backed on top of peer-to-peer network software. I mention these, there are a number of adults in different offices had their computers swept for spyware, and there are just many, many programs there. And how did they get there? It's because their teenagers are out in peer-to-peer networks signing up for file-sharing programs, for music and so on, and maybe that's—put aside the copyright issues, but still, that software is being loaded on your computer and it's there delivering ads to a lot of people who don't' want them.

It's how clear is the consent and can you really get out of these programs? WhenU says it's easy to uninstall their programs. I know some programs which are really hard to uninstall. I don't know how we can do this except by Congress saying that some of this behavior on hijacking computers is unacceptable.

Dr. LEVINE. If I could add a little bit there. Something that's sort of unique about software is that you consent once but then it annoys you forever, which is somewhat different from other software.

Senator BURNS. Sounds like marriage, doesn't it?

Dr. LEVINE. I plead *nolo contendere,* sir. But with most software you install the software and you consent, but once it's installed, it only runs when you tell it to. Spyware is unusual in that it sits there and it gives you, you know, it gives you stuff that may or may not be helpful, you know, whether you ask for it or not. In my case, I don't want Windows to pop up and tell me when I can get cheaper hotels because I know if I want a hotel comparison website I know where to find one.

Senator BURNS. Senator Allen?

Senator ALLEN. Thank you, Mr. Chairman. You know, you all did a great job on spam. My general view though is pop-ups are worse than spam. I had an account set up with Yahoo—huh?

Senator BURNS. It's a form of spam.

Senator ALLEN. It is, but the spam is usually associated with e-mail, and I finally found this e-mail account and said, all right, go in there, use it through Yahoo, it's what I use as my website, or home page. And this is I don't know how many months, there are just hundreds and hundreds of e-mails in there and they were on mortgages, travel bargains, gambling, pharmaceuticals, pornography, whatever all it was, all these e-mails. And it's very easy to get rid of them. You select all and delete and that's it.

Pop-ups you have to click them off. As far as advertising, I like to read the newspapers. I read the *Richmond Times-Dispatch* or the *Post* or the *Washington Times,* whatever it may be, the *Bristol* paper. At any rate, they have advertising for realtors there and whatever other things they may want to advertise, but that's not invasive, that's just on the side of the article. You go on, say, *Buccaneers.com,* they're selling stuff, *Raiders.com, Chiefs.com,* whatever it may be, they're selling things, jerseys and whatever, and that's not a problem, the pop-ups are.

Now, in listening to all of this maybe we can get this agreement from this hearing and why we may need to have Federal legislation in light of Utah. Will you all agree that any legislative approach should establish a national standard, avoid a patchwork of state regulations, and target bad actors, not necessarily harm legitimate online business? Do you all agree on that?

Mr. HOLLEYMAN. Absolutely.

Mr. BERMAN. Yes.

Senator ALLEN. Well, that's where we're going to have to go now. The details of some of these, the definition and so forth, there is that agreement on it. And, of course, Mr. Holleyman, I like your approach, e-spying, ban behavior not technology, that's the approach.

Now, we've heard about all these statistics regarding the amount of spyware on consumers' computers, which is all very disturbing and worrisome. According to Mr. Holleyman, spyware amounts to an abuse of technology. Clearly that is the case. Now, can any of you all share with us and the public what is the technology industry doing to help address this problem? If we're trying to educate the public, what is the technology industry doing to address it, other than dragging some guy who's an expert or person who's an expert to try to stop it?

Mr. BERMAN. There are a number of technologies which are being offered. Earthlink has a spy audit and America Online is also offer-

ing a package which helps users of their services sweep, detect, and eliminate spyware, so there's a technology solution. I know that Microsoft is working on part of those solutions. We've been trying to convene a group of industry and public interest organizations to try and sort out what's being done, what can we do through self-regulation, what can we do through standards, what falls into the need for legislation and can we define bad behavior. And it's, I think it's going to be a mix of all those.

We've also worked on a standard called P3P, which allows companies to express their privacy policies in code, which can be read by a consumer who can set their settings to what they want, and if that was widely adopted, it would be much more transparent to deal with companies like, that promote spyware or adware. You would be able to do a lot of negotiation or at least be able to say this is consistent with what I want as a consumer and say yes or say no.

And so there are technology solutions that are out there, but I think that it's going to have to be a mix of technology, self-regulation, and legislation. But the self-regulation in this area I don't think is going to come until we have some clear standards, and if we have some clear standards, some of it's going to have to be put in the legislation.

Senator ALLEN. Mr. Holleyman?

Mr. HOLLEYMAN. There are technological solutions that are both being made available now and that companies are actively working on for their next generation of products. I agree with everything that Mr. Berman said that a combination of consumer education, technology tools, and best practices that we're eagerly working on with Mr. Berman's group and others. It may well take targeted legislation, and also enforcement of existing laws. I want to reiterate that the status quo is not acceptable. Something needs to be done. It's just a question of how do you then tailor that new legislation to deal with it.

Senator ALLEN. Dr. Levine, what's your perspective of the technologies that are available, and maybe people are not availing themselves of them?

Dr. LEVINE. There are certainly some technologies. There's the programs Mr. Berman referred to. There's also some fairly nice free programs called Adaware and Spybot. But I'm still concerned that it's difficult for consumers to make rational tradeoffs here. I can't tell you how many times I talk to someone, I say, do you believe that your personal privacy online is important? Of course. But then they say, well, you know, would you provide your name, address, Social Security number, mother's maiden name, and annual income in exchange for a raffle ticket for a $5 plush animal, and they all do.

Senator ALLEN. Well, that's——

Dr. LEVINE. Well, and I realize we can't keep people from being naive, but I think people don't appreciate sort of the value of what they're giving away and the risks they're entering into. So, I realize none of us are interested in having a nanny state here, but I do think that it's important to recognize the value of the data these things can collect and I think it's reasonable to put some fairly strong hurdles in the way of saying, you know, do you really want

to give this up, is what you're being offered really valuable enough to be worth this exchange?

Mr. BERMAN. One point on that, which is that the risk involved and the tradeoffs, sometimes consumers are given the opportunity to get a free program or free service in exchange for signing up for an adware program which is essentially downloaded on their computer, but they're not necessarily up front, and this is something that SPY BLOCK tries to deal with. They're not given up front any knowledge of what that adware program is going to do and how many ads and how intrusive it's going to be and when it's going to come, so they're signing up without real knowledge of what they're getting into. Maybe that's solved by the ability to uninstall, but uninstall is——

Dr. LEVINE. No, because once you've given your data away, since the U.S. has no tradition of strong data protection laws, once somebody's collected your data, they've got it, and if they then transfer it from place to place to place, we all know stories, we've all heard stories about somebody who disclosed information one place and it ended up someplace really much worse and far away.

Mr. BERMAN. Well, I put those in box one, which are privacy violations. There are also ad services who are not collecting information, and I want to make clear that they raise a problem. Even though they are not violating privacy, they are raising issues of user control over their computer.

Senator ALLEN. Mr. Naider?

Mr. NAIDER. And we are trying to address it, I guess, at a slightly different angle, which is economically. We've put together what we call our five points definition of what is the difference between legitimate adware versus spyware. Interestingly enough, adware used to be a positive word. We put out press releases 2 years ago talking about our own adware. I wouldn't think of putting out a press release today mentioning adware in conjunction with our product because it's become a loaded word because there are some folks that claim they're adware and actually are spyware.

We've actually put out a definition that we're trying to promulgate within the industry, and that definition has five points, and point number one is the disclosure. When you initially install it, it has to be visible, right in front of the user, that the presence of additional software is something that if the user takes the time to read is visible, it's not buried six pages down in a license agreement.

The second thing is that the license itself for this type of technology needs to be clear, concise, and understandable. We use a two-page license agreement to the dismay of our lawyers because we basically said that anybody who reads a license agreement should be able to understand it in 5 minutes. We think the second point is the disclosure of the license agreement and making it clear and concise.

The third point is the branding, specifically if you display Windows or add Windows such that consumers don't wonder why I am seeing this ad, whether they may like it, like Dr. Levine—they may not like it like Dr. Levine or like it, like some other folks, it should be very clear where it's coming from, why it's there, and who is delivering it.

The fourth point is ease of uninstallation. Consumers that don't want the software should easily be able to uninstall it, should make a choice. With respect to what the Senator mentioned before, there is actually a big difference between spam and legitimate desktop advertising software. Actually I've tried many times to stop spam to my office mailbox. I can't do it. But if you want to uninstall software that's legitimate software, it's actually easy to uninstall it. So if you abide by that fourth point of uninstall, then we consider that in keeping with this philosophy of being adware and not spyware.

And the fifth thing is privacy protection, which is, regardless of whether you get disclosure, regardless of whether you get a license, regardless of whether you brand and you make it easy to uninstall, if the practices that you're doing involve keystroke logging, collection of personal information, then it doesn't matter that you got all this because there may unwary consumers that agree to it.

So we believe that by putting out this five points of what defines legitimate desktop advertising versus spyware, we can actually create a definition where those who claim that they're doing legitimate advertising were actually spyware don't survive economically, because the advertisers who use it basically say, are you adhering to these five points, are you doing this legitimately, and if not we're not going to spend money with you. And that's our approach and we actually hope that this type of legislation will look at these different pinnacles of disclosure, license, branding, uninstall, and privacy, and be able to set that standard as well for the market.

Senator ALLEN. Are you saying, final question, I'm like Dr. Levine. If I want to figure out how to get a flight from one place to another, again, Yahoo will have Travelocity linked up with it or whatever. There's a—you can find it, you can search and find it without somebody saying, here, you can be on a cruise or you can get these discount rates and so forth. I'd just as soon not have to click them off and have them covering up what I'm trying to read.

Now on your—you seem to have some standards, those don't, which make a great deal of sense. Let me ask you this though. How easy is it for someone to remove on your software? Say there's someone like me or Dr. Levine who, I don't care, it is good to know where it came from, the source of it is good, that obviously would be wonderful as a way of knowing the source or you can figure out how they got your name and then blame them rather than some of the deceptive things, you think it's coming from AOL or Microsoft when they have absolutely zero to do with it. And you see AOL or you see Microsoft and it connotes a certain credibility and credence, so I think it's great to have that tracing.

But how easy is it, or how would someone who doesn't want to get your advertising through WhenU.com, how easy is it to remove it?

Mr. NAIDER. I think the numbers speak for themselves. We've done over 100——

Senator ALLEN. I missed your testimony, so I'm sorry if you've already said this.

Mr. NAIDER. That's OK. We've done over 100 million unique installations of our software and initially about 50 percent of people kept it and now 80 percent remove it. Now, that's a challenge for

us. Part of the reason that they remove it is because there are so many other programs not adhering to standards that they just get an Adaware program and everything gets removed.

But the answer is, it's very easy to remove. It can be uninstalled through your control panel add/remove, which is the standard way for uninstalling software, and more importantly, each ad unit tells you directly how to get information about uninstalling where it says, go to your control panel and do it.

So the empirical evidence is that it's very easy to uninstall, and as a result, we freely acknowledge that there may be consumers that don't want to see a coupon when they're about to shop and don't want to see, but to the extent that there are consumers that do and that it's quite beneficial to either have that software for its own merit or maybe you're willing—maybe you don't want to see it but you're willing to see it because you get a free sports ticker program. There are many consumers like that. They decide, well, I don't necessarily love the idea of seeing a coupon or a free travel ad, but you know something, I get a free sports ticker, so I'm happy to do that.

We want those consumers to have that choice. By following these types of standards, you give the consumers a choice. By making any unilateral decision one way or the other, you don't give them the choice, and we hope that that's what this legislation accomplishes.

Senator ALLEN. Understood. How many others in your business have the facility of removing pop-ups that you all do?

Mr. NAIDER. It varies dramatically. There are others—we are certainly the leader in the industry in terms of the standards that we set and there's a full spectrum of activity from folks who don't necessarily adhere to every one of these points, maybe four or five, to folks who absolutely make it impossible to know that—or do their best to make the consumer unwary that they've installed it, once it's on the desktop, no branding, no idea that these pop-ups might be coming from software, no easy way to uninstall.

So the answer is that there's a full spectrum of activity and we hope to combat it both through, you know, we hope that your efforts, as the Chairman and the Senators of this Committee through legislation will combat it, and our efforts from the standpoint of market education will allow certain models to emerge and to develop and to meet what ultimately can be very, very, very pro-consumer, pro-competition, pro-comparative advertising type of standards and other models to disappear, so that the experience, the nightmare experience that people have, and I've heard this many, many times, you know, the nightmare experience that you have is I have 12 things on my computer, I have no idea where they come from, I don't know how to stop them. We want to see that disappear as well.

Senator ALLEN. Thank you, Mr. Naider.

Senator BURNS. Mr. Holleyman, I referred to a while ago, do you think right now there are enough laws on the books with regard to privacy that we could deal with this SPY BLOCK or spyware without passing this legislation?

Mr. HOLLEYMAN. There are laws related to deceptive advertising through the FTC Act, the Computer Fraud and Abuse Act, all of

which can be applied and should be applied, and I am very much holding open the possibility there may need to be additional legislation that's behavior-based to close the gaps.

Senator BURNS. Would you agree with that, Mr. Berman?

Mr. BERMAN. I agree that we're going to need legislation to close the gap because there is—we need to look at where it's clear hijacking of computers and not allowing you to uninstall and taking over your Web page and a lot of behavior that's in our FTC complaint against a company or two. We may need to—existing law may cover it, we need to try and figure out where it falls short and come back and fill in the gaps working with you.

With respect to the privacy issue of collection and dissemination of information without notice and consent in this area we need legislative standards.

Senator BURNS. Whenever you start talking about national standards and this type thing, we ran into something in spam and I think that we should also look at it, because with our visits with our international friends, this just isn't a national problem. In other words, everything that this spyware can be installed from not necessarily friendly soil, so to speak.

Do we need to work with our international partners to also craft legislation that would work in their countries and recommend they do so?

Mr. BERMAN. I would recommend that we try and sort this out first.

Senator BURNS. Here?

Mr. BERMAN. Here. And so that we know, maybe we have some consensus about what we're talking about. Right now it's a tower of Babel as far as I'm concerned. I mean, what's in and what's out? But I think if we get down to some bad behavior, which is like CAN SPAM, let's get some real things that we, you know, *res ipso locutor,* the thing speaks for itself, we understand it, this is bad, let's get it. Then I think we can begin that dialogue.

I agree that this is not something that because we pass a law it's going to be solved, because spyware can be served from overseas. That's why, you know, ideas like a do-not-spyware list won't work, I mean, because we're dealing with a global network. That's why we need technology solutions as well as——

Senator BURNS. Yes, sir.

Mr. HOLLEYMAN. Can I make two points on that? One, we were of the view that a behavioral-based approach would give us the quickest, fastest tools in this country to try to address the problems. Second, because we work as BSA on a global basis on public policy laws, I think there is a reason to look carefully at trying to avoid having to define what software looks like and what technology looks like, because if we adopt that approach in the U.S. rather than the behavioral approach, presumably we're going to be asking all of our major trade partners to pass similar legislation that defines the way software looks, and the same technology that can be used for bad purposes for spyware may provide good future uses of technology in areas like diagnostics and security tools.

So if we can avoid having to create here and then around the world a definition for how we create software and deal with the behavioral approach, we think we'll be better off.

Senator BURNS. You see, it's my thought on this thing that Mr. Naider is in a legitimate business. He is a legitimate operator and entrepreneur and runs and business and I think the standards are very important, because if we get the bad guys out there doing bad things, it does bad things to you. You get a bad reputation, and that's what we want to do is for the industry to come together. Basically that's what we did with spam is it forced industry to sit down and talk to another and say, OK, how are we going to deal with this, and then they said, yes, we need a law, and yes, four of the biggest ISPs there is in the country filed a lawsuit on some of these people who are really basically clogging their pipes. In other words, they just can't handle everything that they throw at them.

So most everybody else has answered my question. I've sat here very interesting, but I do want to work with all of you—you had some other—you got a another question? A couple more, OK. With respect to how we define and to see if we can't do the same thing with this legislation as we intended with CAN SPAM, is the industry has to come together to the table and help us with those standards. You can't let government set the standards. If we do, we'll be locked into technologies.

I can remember first, when I first come here, we flew out to the consumers electronics convention in 1990 to Las Vegas and we were going through this debate on who's going to standards for high definition television. And there were some people out there very well-intended that says government has got to set the standards. And I said, if government sets the standards, then we're going to be locked into that because it's hard to change and technology moves too fast, that if government sets it, then we're locked into that situation.

So we want to work with you very, very closely on definitions and allow the industry to come together and to really identify the bad guys and help us a little bit, because self-policing effect does have a cooling effect on those people who would do bad things. Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman. You have really spoken for me in that regard. I think you've laid out the challenge very well. We're going to need to work closely with all the people at the table if we're to move this and that's what we've tried to do so often in the past and I appreciate your making that comment.

Just a couple of clean-up points that I'm interested in in terms of where we go. As you all, I think, have picked up, as Senator Burns and I have really had a little bipartisan island here where we have tried to kind of prosecute these causes that obviously are complicated and technical and sort of learn as we go, and I sort of sense a little bit of a reversal of position in terms of you, Mr. Holleyman. I just want to kind of make sure I'm sensing this.

When I see your suggestion that Congress, and I quote here, simply prohibit the distribution in interstate commerce of user information obtained electronically from an individual's computer unless the person seeking to sell the information can show it was collected with the user's explicit permission, and explicit would obviously be a definition, that certainly raises the prospect of your organization supporting a general online privacy bill.

Now, that's something that you all have been concerned about in the past and have wanted it to be much narrower, but I suspect that as this gets more complicated and we deal with the state and Federal issues and states going off on their own, people naturally are going to start to look at this differently without going into all of the issues that that statement raises about whether it apply only to software downloaded to a user's computer or to websites a user visits, there's score of issues.

Are you all moving generally in the direction of a general online privacy bill?

Mr. HOLLEYMAN. We're not in a position at this point to raise a general online privacy bill. We do think that there are very legitimate privacy issues that are being addressed in part in the marketplace today and for most online experiences. But what we do think is, specifically, with regard to spyware is what we need to do is create a mechanism that dries up the market for information that's obtained and exploited commercially, where there is not a clear understanding that such information can be sold and distributed.

Senator WYDEN. I won't belabor this, but other than the definitions about explicit permission, that sentence I read sure sounds like the predicate for a general online privacy bill, which takes us back to Burns/Wyden 1 and would, I think, be very much worth pursuing. Chairman Burns and I have done all of this in total lock step along the way, but we tried this years ago and I personally would be very excited if you and Mr. Berman possibly could guide the Committee back to what Chairman Burns and I tried to do years ago. We're going to try and get this bill passed because I think we've seen tremendous unhappiness, but I'm sort of trying to, with all of you here, to sort of lay the groundwork, because when I read that sentence, it struck me, and I haven't compared your testimony and everything else. That that was beyond where you all had been in the past and was sort of encouraged about the possibility that we might get the two of you to be a bulwark for—look at Jerry, he's——

[Laughter.]

Mr. HOLLEYMAN. I'd be happy to talk about this any time.

Senator WYDEN. I won't belabor it. I was encouraged by it. One other technical kind of question, a security question for maybe you, for Dr. Levine and Mr. Berman. We haven't talked a lot about it today, but certainly this issue of security risks with respect to downloaded software, I mean, even if the software isn't malicious, isn't is possible that well-meaning software could, in effect, leave the back door open, making the computer more vulnerable to viruses and hackers?

Dr. LEVINE. It happens all the time.

Mr. BERMAN. In fact, it's the vulnerability of computers that some of these spyware programs are exploiting, back door vulnerabilities and creating security breaches of their own, so that's something that we have under study and which this working group is looking at, but it is certainly one of the reasons why, one of the motivating reasons why we have to think about really closing these loopholes and closing this problem down.

Senator WYDEN. That struck me as something that really hadn't been mentioned, but we're going to think of this primarily as something that's intrusive and violative of those who own computers, but also strikes me as opening up a real glide path for bad guys and an opportunity to have some real security vulnerabilities.

Dr. LEVINE. I think a lot of what these programs do now should be, probably is illegal already under—in computer tampering laws, and it's possible that it might be useful to have a statute that makes it more clear that this particular kind of tampering is what you contemplated in the existing tampering acts, so each case doesn't have to come through and sort of educate the judge and say this sequence of events means you broke this law.

But in general, yes, the security problems on users' PCs are enormous and spyware jumps through some of them and causes others.

Senator WYDEN. Mr. Chairman, excellent hearing and I'm looking forward to working with you and like we've tried so often to sort of begin another journey and I look forward to doing it with you.

Senator BURNS. Well, and this may take more than four—I hope it takes less than 4 years, but at least we're started. I want to reiterate that SPY BLOCK requires notice and consent for four types of potentially damaging software, software which collects information about consumers and transmits to third parties over the Internet, adware providers are required to tell consumers what types of ads will pop up on users' screen and what frequency, Software that modified user settings like changing their home page and software that uses distributed computing to use part of the computer processing power in the background.

You know, we've all time—Mr. Naider, and just one follow up and I thought about, you've given us a good scenario on your business, legitimate, run professionally. Give us an example of when you go too far. In other words, just give me an example.

Mr. NAIDER. I'd be happy to.

Senator BURNS. Just for the record.

Mr. NAIDER. Be happy to. A consumer installs a piece of software in the course of installing some other piece of software where there's absolutely no visible disclosure, there's some disclosure buried perhaps six pages deep in the license agreement. Once on the desktop, there's no visible indication to the consumer that they have that piece of software, whether it shows ads or not. It may show ads, whether it's pop-ups or other types of ads, but there's absolutely no indication to the consumer that those ads are coming from software. The consumer just wonders. Or if it doesn't show ads, the software captures things like personal information or keystrokes or zip code location, et cetera. And then the consumer is not given any information about the software or how to uninstall it.

These are things that we see every day in our business and we know that it exists and there's a full spectrum of activity and we believe that that type of activity needs to be curtailed for the health of the industry, for the health of consumers' computers, for the health of the industry as well.

Senator BURNS. Well, I know identify theft and of course credit card numbers are worth lots of money.

Mr. NAIDER. Absolutely.

Senator BURNS. And that's where the bad guys come in. Thank you for your testimony today. We look forward to working with all of you. We're going to leave the record open for the next 2 weeks and if there are questions from the other members of the Committee, please respond to them and the Committee. Thank you for coming today and these hearings are closed.

[Whereupon, at 4:07 p.m., the hearing was adjourned.]

○

This page intentionally left blank.