S. HRG. 109–1090

SPYWARE

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

MAY 11, 2005

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

U.S. GOVERNMENT PRINTING OFFICE

61–887 PDF WASHINGTON : 2010

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

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

TED STEVENS, Alaska, *Chairman*

JOHN MCCAIN, Arizona
CONRAD BURNS, Montana
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
GORDON H. SMITH, Oregon
JOHN ENSIGN, Nevada
GEORGE ALLEN, Virginia
JOHN E. SUNUNU, New Hampshire
JIM DEMINT, South Carolina
DAVID VITTER, Louisiana

DANIEL K. INOUYE, Hawaii, *Co-Chairman*
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
BYRON L. DORGAN, North Dakota
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK R. LAUTENBERG, New Jersey
E. BENJAMIN NELSON, Nebraska
MARK PRYOR, Arkansas

LISA J. SUTHERLAND, *Republican Staff Director*
CHRISTINE DRAGER KURTH, *Republican Deputy Staff Director*
DAVID RUSSELL, *Republican Chief Counsel*
MARGARET L. CUMMISKY, *Democratic Staff Director and Chief Counsel*
SAMUEL E. WHITEHORN, *Democratic Deputy Staff Director and General Counsel*
LILA HARPER HELMS, *Democratic Policy Director*

CONTENTS

WITNESSES

APPENDIX

SPYWARE

WEDNESDAY, MAY 11, 2005

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

The Committee met, pursuant to notice, at 10 a.m. in room SR–253, Russell Senate Office Building, Hon. Conrad Burns, presiding.

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

Senator BURNS. We will call the Committee to order—I know the witching hour is here. I would like to get started on time, because we sure won't make up any time later on during the day. I welcome everybody here today.

We are here to discuss the growing problem with spyware. Even though Chairman Stevens can't be here today, I'd like to thank him for calling this hearing, and allowing us to proceed to address all the challenges that we face in the computing industry today. It's my pleasure to be joined by our witnesses. Mr. Hughes of the Network Advertising Initiative, Mr. Moll with Webroot Software, and Mr. Schwartz with the Center for Democracy and Technology.

Over the past few years, we haven't always been able to work in Congress with folks like yourselves that have been critical to our success in managing the booming communications infrastructure, so I thank you for your time, and for being here today.

Spyware is an increasingly worrisome threat to our every day activities in cyberspace. Spyware refers to software which secretly collects information about computer users and shares it with others over the Internet without those users' knowledge or consent.

This sneaky software is often used to track the movements of consumers online and even steal passwords, social security numbers, bank account information, and other highly sensitive personal data. Spyware can also be used to turn a person's computer into a tool that participates in criminal activity directed by a third party.

The problems posed by spyware, and to the security of cyberspace in general, are thus real and they are urgent. As was the case with spam several years ago, I believe the solution lies in the right mix of technical solutions and tougher legislation. Both will be necessary to make a meaningful dent in the quantity and the types of malicious code that get downloaded into the private computers of businesses and citizens, without their consent. However, we also have to be careful not to throw out the baby with the bath-

water, by making many ordinary and positive types of online business' practices illegal. The area of adware in particular is an important gray area to keep an eye on. How exactly are online advertisements served up to the users, and what kind of consent is most appropriate? Most adware models are good for cyberspace because it's important to have a robust and responsive advertising component for most commercial online services. I, being an old broadcaster, understand that.

But when it comes to installing software on private computers, we have to make sure we don't allow some of the more unscrupulous players out there to spoil the field for all the good actors who are just trying to make cyber businesses more efficient.

As many of you are aware, Senator Wyden and I have been working on an anti-spyware bill for more than a year now, in fact 2 years, to be right honest with you. The underlying principle of our legislation is that a person should have the right to know what is happening to his or her own piece of property. I also would like to thank Representatives Barton and Bono for their continued efforts on this issue in the House of Representatives. Their approach is similar to ours, and we look forward to working together with them in the future. The Spy Block bill, S. 687, that we now have in front of us includes a great deal of industry and consumer group input, and we believe it to be a major step toward a resolution of the problem at hand.

In the 108th Congress a similar version of that bill was marked up out of this committee unanimously. Given the combined effort involved, Senator Wyden and I truly are hopeful that we can do it early this session. We also have the input of Senator Allen and many other folks who are deeply interested in this issue. We plan to work with everybody on this committee to get a product that we all can be proud of, but also a product that gets the job done.

As we review these issues, it's important to understand that a person's or business's computer should be viewed as private property and that the rightful owner should be able to control access to it. In the same way that you should have the right to authorize access to your home for maintenance or upgrades, you should have the right to control who installs software on your computer.

So, I thank you very much for coming today. And now I will call on Senator Smith from Oregon if he has a statement.

STATEMENT OF HON. GORDON H. SMITH, U.S. SENATOR FROM OREGON

Senator SMITH. Thank you, Mr. Chairman. I appreciate your holding this hearing. It's a very important topic. I share your concern on the issue. I have a keen interest in spyware, and have continued to work on these issues to protect consumers and businesses.

I was stunned to learn that according to a survey by the National Cyber Security Alliance and America Online, 80 percent of all home computers are currently infected with spyware. Furthermore 80 percent of the owners of infected computers are not aware their computers are, in fact, infected. Nonetheless consumers are clearly concerned about the issue. Consumers have downloaded free

versions of two of the most widely used anti-spyware programs over 45 million times.

Although spyware has been used for many deceitful purposes, including theft of personal information from infected computers, the technology behind it has been used toward legitimate ends, as well. The complete regulation of an entire category of technology or product can have many unintended and serious consequences.

If the definition of spyware becomes too wide, legislation adopted in haste might not take into account the evolution of future technologies and, in turn, stifle innovation. I believe we need to limit the abuse of the deceitful practices by dishonest users, but at the same time, allow industry the ability to build on, and improve, existing technologies. I'm aware of several technologies that we learned from Mr. Gates the other day, that was very encouraging. To that end, I am working with Senator Allen to develop legislation that increases the FTC's current authority to enforce existing laws and allows the agency to also coordinate with law enforcement overseas, to prosecute deceptive online activities.

We need to give the FTC the necessary tools to go after the individuals who are already violating current Federal law. I agree that we do need to address the most egregious activities and behaviors without placing unnecessary restrictions on the entire technology industry. I also believe that an appropriate balance can be found between limiting the legitimate use of existing technologies, and allowing for the technology industry to grow, expand and innovate.

As we continue to address this issue, Mr. Chairman, I look forward to working with you and all my colleagues on this committee to find the right balance in a timely manner. Thank you.

Senator BURNS. Senator Allen?

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

Senator ALLEN. Thank you, Mr. Chairman, and I thank you for calling today's hearing, and thank all our witnesses for appearing this morning as well.

Since the last time the Committee considered this issue, consumer complaints and concern about this irritating, volatile spyware issue has increased, with only a few consumers figuring out how to combat it. As Senator Smith stated, the AOL and National Cyber Security Alliance, in October of 2004—I won't repeat his statistics—but the average computer had more than 90 spyware programs on it. Dell Computer said by the end of 2003 they reported that spyware was the number one consumer complaint coming into their call centers. Most alarming, last year nearly half of online identity theft cases were caused or initiated by some sort of spyware program.

All of us can agree that under no circumstances is it acceptable to deceptively monitor a consumer's activities online. In fact, false and misleading practices associated with spyware threaten consumer confidence and harm the Internet as a viable medium for communications, and electronic commerce. In examining this offensive spyware issue which causes aggravation—it insults some people and some of the adware in particular—and additionally you get degraded computer performance. I believe we need to encourage, to

the greatest extent possible, market-driven technology solutions, as well as strengthen the enforcement of existing Federal laws.

Every legitimate business associated with the Internet, in my view, has an interest in eliminating spyware. A recent FTC, or Federal Trade Commission, report suggests that the rapid technology advancements being made to combat spyware such as fire walls, filters, anti-spyware tools, improved Internet browsers, and operating systems are constantly providing newer and more affordable protections to consumers whether at home, or at the place of business. The Internet's viability depends on consumers' satisfaction and consumers need to be made aware of these advancements, so they can be protected from harmful spyware applications.

Because the fraudulent and deceptive installation of spyware programs is presently a violation of Federal law, such as the Federal Trade Commission Act, and the Computer Fraud and Abuse Act, Congress must focus its efforts on adequate resources and penalties to combat the problem. Federal officials believe they already have adequate authority under existing statutes to prosecute spyware purveyors. Law enforcement is not stymied by the lack of Federal jurisdiction, but rather from the lack of overall resources. That's why today I'm introducing legislation with Senators Smith and Ensign, which would provide Federal law enforcement officials with the resources and tools necessary to increase the breadth and strength of anti-spyware enforcement efforts. Our legislation strikes the careful balance of pursuing illegal, wrongful behavior, while not stifling or limiting technology innovation or legitimate online transactions.

Specifically, since spyware violators are not limited to state or national borders to perpetrate their illegal activity, the legislation will set a national standard for the unfair and deceptive practices associated with spyware. Additionally, our legislation will provide the Federal Trade Commission with authority to share and coordinate information with foreign law enforcement officials to improve their ability to bring cases and prosecute international spyware purveyors. Last, our legislation addresses the most egregious activities and wrongful behavior conducted via spyware by significantly increasing the civil and criminal penalties, including disgorgement. In other words, get after the ill-gotten gains of these criminals.

Mr. Chairman, I really look forward to hearing our witnesses opinions on such an approach, and as I indicated, I would prefer a market-driven solution, but believe Congress can take an active role, in aiding law enforcement officials and providing adequate resources to combat this problem, while also increasing and toughening the penalties against such illegal activity. I would actually like the disgorged profits, proceeds, these ill-gotten gains to be used to actually fund further prosecution of spyware purveyors. And I look forward to working with you, Mr. Chairman and Senator Burns, because you've shown great leadership on this effort, and the rest of the Committee, we do need to work to address these concerns raised today.

Thank you.

Senator BURNS. Thank you very much. Mr. Nelson?

STATEMENT OF HON. BILL NELSON,
U.S. SENATOR FROM FLORIDA

Senator NELSON. Mr. Chairman, I am delighted to be a co-sponsor, along with you, Senator Wyden who's sitting right out there in the front row, and Senator Boxer on this Spy Block Act, it is most, most important. It's interesting that this hearing is being held the day after we just had the hearing in this very same Committee on ID theft. And all of this, all of these problems are converging at once because of the advance of technology, that people are stealing our identity, people are intruding into our computers, and one of the things that's happening in that intrusion of computers, be it by phishing, or be it by surreptitiously putting a program in, that they are starting to poison the minds of our children. When suddenly up flashes this Internet porn site. And so, this is an extremely important hearing that we are having, the legislation that we filed is extremely important. Just like yesterday's hearing on what we are going to do about people stealing our identity.

It's not like you could go out and shred anything that you were throwing away, or put it in a burn bag, because all of this information is in cyberspace now. And the sophisticated thieves penetrating that can virtually take over our identity, and that's the subject of this hearing, they can absolutely penetrate into the most private domain that we have, which is our home, and suddenly implant stuff that we don't wish to have implanted. And so I am really looking forward to this hearing.

Senator BURNS. Thank you very much. There's an old farming term about that. It is the harvest by unscrupulous folks. And that's what we have here. Senator Boxer?

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

Senator BOXER. Thank you so much.

I want to also welcome Senator Wyden who I see there. We miss you on this committee, but we know your interest remains. I'm very happy to see you here.

Mr. Chairman, thank you for holding this hearing. I was proud to join with you and Senator Wyden in reintroducing the Spy Block Act, which I now am happy to know that Senator Nelson is a strong advocate of. Our legislation is designed to address increasing concerns that I have heard coming from California, and other states, about spyware. These insidious programs install themselves on computers without the users giving permission or even knowing about it.

It's hard to use analogies with this, but it is sort of like somebody walking around your house invisibly. You think you can use your computer to read whatever you want to read, whatever you want to access, you access. But with spyware someone is out there gathering personal information—your passwords, your e-mail address—and sending it over the Internet to anyone they want, including maybe criminals. They can monitor the sites a computer user visits and send targeted pop-up ads, such as that described by my colleague, Senator Nelson. They can change a computer's home page setting, to that of the spyware's choice, or they can redirect

a user's Internet browser to go to a different site than the consumer intended.

In addition to privacy and security concerns, spyware and adware programs can cause computers to crash, disconnect from the Internet, and interfere with legitimate software programs. And, as Senator Nelson said, spyware companies target kids. One application called BonziBUDDY creates a purple ape that swings across the computer screen, telling jokes, singing songs, and delivering voice ads. Children often download such programs and the parents have no clue as to what they really do, and the children have no clue as to what the spyware does. The FTC successfully pursued Bonzi software for violating the Children's Online Privacy Protection Act, but that has not stopped companies from producing and distributing spyware.

The point is, having a law to crack down on folks is good. I have no problem with it. But I think we have to do more than that, because clearly it's still going on even though there have been lawsuits filed. The problem has grown to epidemic levels, it's estimated that the market for ads delivered or generated by adware is currently worth $2 billion a year.

Last October, America Online and the National Cyber Security Alliance examined the computers of 329 randomly selected Internet users, and found that 80 percent of them contained some form of spyware. The average infected computer had more than 90 spyware and adware programs. This trend must be stopped. It harms consumers, damages computers and undermines the privacy that people expect and deserve, and it goes after kids. And I think if anything unites us on this committee it should be that.

Our bill simply says that all software makers, including spyware makers cannot sneak onto your computer. Specifically, the Spy Block Act prohibits the installation of any software without the 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.

Some people have objected to our bill, saying it should focus only on spyware and not on all software. The problem is that nobody thinks the software they produce is spyware. That is why our bill covers all software; otherwise the people who produce spyware will simply try to define themselves out of the category by claiming that their particular software is not spyware, and imagine a court case on that.

Consumers deserve to be protected. Software should not track a person's activities and that of his or her family. That's Big Brother. That's Big Sister, and that's what we have to stop. And I would hope my colleagues on the other side who may not be for this bill will understand what we are talking about here. We are fighting for the individual over an organization that wants to spy on them. So, by applying common principles of consumer rights for all software, we deal with the spyware problem and enhanced consumer rights on the Net.

Mr. Chairman, I hope we can get this bill done, and I look forward to working with you, Senator Nelson, and the others on the Committee. Thank you.

Senator BURNS. I thank Senator Boxer.

We have been joined, among our very, very capable staff on both sides of the aisle by a new staffer this morning, and we would inquire whether the new staff member over there would like to make a statement at this time.

Staff Member: No, thank you Mr. Chairman, but your graciousness is appreciated.

Senator BURNS. I would appreciate the status report.

And we're also joined this morning by Senator Wyden, who is no longer a member of this committee, and was a very good member of it, and we worked on many issues, and of course we've worked on this one for a couple of years. We welcome him back this morning for a short statement. Welcome back, Senator Wyden.

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

Senator WYDEN. Thank you very much, Mr. Chairman.

First of all, I want to prove that contrary to everything that is said in the media, not every Senate speech has to be a filibuster, so I am going to be real short this morning and just give a couple of thoughts. A lot of you, I think, got the sense that I still wish I was on the other side of the desk with you.

Senator BURNS. You are welcome to join us at any time.

Senator WYDEN. That's a very kind offer, and I thank you very much for it. I think there are the makings just in the opening statements that I heard of a very good bipartisan agreement, between you and I, Mr. Chairman, Senator Nelson, Senator Boxer, and Senator Allen, who makes a lot of sense, too, in terms of talking about tough penalties. I think clearly there are all the makings for a very good bipartisan compromise.

I would just say, the last time out the major effort made was with respect to spam, and this is a much more serious problem. With spam you can hit the delete button, but with this stuff it crashes your system. And, so people now don't know where it comes from, don't know how to wipe it out, and this is, I think, a much more serious problem and my colleagues essentially touched on that.

I am particularly troubled about the fact that it really stems, as a spider web is created in our computer systems, from the fact that we've got to figure out how to protect people doing innocent work and innocent businesses, from those who cross the line. Much of the spyware and unwanted adware travels, essentially, as imposters via legitimate Internet advertising. What happens is companies enter into the advertising arrangements with legitimate Internet ad buyers, who then go out to advertising networks that can use thousands of affiliates, sometimes 70,000 affiliates, some of which are not legitimate. This array of affiliates are paid, in effect, by the click, and therefore have an incentive to rack up the largest number of clicks where the rogue software originates. I thought it was well described—and Senator Boxer's been a great advocate on these issues—by the *Los Angeles Times* just a few days ago, they said, "if an affiliate slips a deceptive piece of software into somebody's personal computer and persuades the owner to buy something, the transaction can then be passed to three or four businesses, each of

which take a cut before the affiliate network hands off the customer to the merchant.

That is, in effect, how the cyber plague can grow exponentially and produce the figures that several of you touched on, and I was especially pleased that several colleagues essentially described the drive-by download, which also can be—in many instances—how this originates.

I'd would start by just outlining six principles I think could be the basis of a bipartisan law bringing together my colleagues. First, let's make sure that consumers are in charge of their computers, not some company that they want no part of. And you can start by banning drive-by downloads.

Second, when somebody jumps on their computer they should not be exposed to a Coney Island full of hucksters where they get tricked into installing software that they don't want, or where they can't identify the source of the ads. So, let's make sure the consumer is informed about who is providing the software. I think this touches on a point you and I made continually, Senator Burns, with respect to the spam debate. People in this country ought to have a First Amendment right to communicate, but they also ought to have a First Amendment right to tell folks to stop and a prerequisite to doing that is making sure they can identify the source of the ads.

Third, it seems to me no software should allow any ad or information collected at one website to travel with the users to another website. You stop that and you get at this problem of the affiliates that I touched on.

Fourth, consumers need to be able to remove or disable any software they don't want, so that when software is installed on a computer it should not be an irreversible act, and I think technologically that's a possibility.

Fifth, to pick up on the point that Senator Allen made, we ought to come down on the offenders with hob nail boots, that means using the Federal Trade Commission, the states Attorney General—I know that Eliot Spitzer brought an action just a couple of days ago to indicate that the states want to be good partners in it, and I support Senator Allen in that effort.

Finally, I would say that we ought to protect the companies that—in good faith—try to help consumers get rid of these cyber plagues, and they ought not be scared out of business simply because they are trying to do the right thing. You have to draw a clear line between legitimate advertising and what happens when the spider's web gets created through the affiliates, and the various approaches that end up junking our system full of all of this trash that really can crash the entire system.

Mr. Chairman, you are kind to let me come, and if I had my way I would be up on the dais with all of you. I am just looking forward to working with you and based on the opening statements I think this is there for the doing.

Senator BURNS. Well, you are welcome to join us up here if you'd like, and stay for awhile.

We are going to start the discussion this morning, and I think that's what we want to do. We've got several representatives, stakeholders in this issue, and so we will start with Trevor Hughes

who is Executive Director of the Network Advertising Initiative. Mr. Hughes, we appreciate you coming today, and we look forward to your testimony. If you want to shorten your testimony up, your full statement will be made part of the record. And thank you for coming this morning.

STATEMENT OF J. TREVOR HUGHES, EXECUTIVE DIRECTOR, NETWORK ADVERTISING INITIATIVE

Mr. HUGHES. Thank you, Senator Burns.

Senator Burns, members of the Committee, good morning. My name is Trevor Hughes; I am the Executive Director of the Network Advertising Initiative.

The NAI is a cooperative group of online companies dedicated to addressing public policy issues that occur at the intersection of issues of privacy and technology, and online marketing and advertising.

In the past, the NAI has successfully launched self-regulatory programs dealing with issues of online targeted advertising. We have also developed programs for the use of web beacons, we have been active in the e-mail and spam debates, and I have had the pleasure of testifying before this committee previously on issues of spam.

Our members, over the past year and a half have turned our attention to the issue of spyware. What I would like to do this morning is present to you two dystopian visions of the future. And, these two dystopian visions of the future are directly related to our actions over the coming months.

The first vision is that we allow spyware to continue to proliferate. And that would, in a sense, pollute the online world to such a degree as to make both e-commerce and the consumer experience online really not successful, and ultimately a failure. That is a bad result for all of us on this panel, for all companies involved in the online economy, and for most importantly, consumers. So, the first dystopian vision is spyware proliferates. And the members of my organization, and consumers, all suffer.

But the second dystopian vision is similar to the statement from Senator Burns. And that is that our response to spyware is too extreme. That we throw the baby out with the bath water. And what I would like to offer today is the good work of the NAI and our pledge of support, to hopefully find a middle ground. I would like to suggest that it's my job, our members' job, and really the work of Congress to find a way between those two dystopian visions of the future, one in which spyware proliferates, and another in which the responses to spyware are so extreme as to limit the very thing that we're trying to protect. That we find that way to both protect the consumer experience, but also protect legitimate online enterprise.

I think most importantly, spyware represents an erosion of consumer trust. This erosion of consumer trust in the wake of spyware is a serious problem for all companies in the online marketplace. Put simply, spyware threatens the economic foundations of E-commerce. And I think I could link arms with my fellow panelists today in making that statement.

As a result, the NAI supports strong legislative and technological action against spyware. Our members cannot thrive in an environment where consumers do not or can not trust the businesses and websites that they encounter on web. However, our members have found that many of the spyware solutions that have emerged are creating troubling collateral damage. In other words, some of the solutions to spyware have harmed the very thing we are trying to protect. The power, the depth, and the free content of the Internet. Our responses to spyware must carefully balance our need to aggressively meet the threat, while protecting the continued legitimate use of the channel.

For this reason, the members of the NAI strongly support Federal preemptive spyware legislation. We clearly need stronger legislative responses. Federal legislation that preempts State laws and creates a single, uniform national standard will both address the threat, and provide a clear set of standards for the online marketplace.

But Federal spyware legislation must carefully balance these needs for aggressive responses against overbroad solutions. Under some of the bills that have been introduced, ubiquitous and important technological tools have been affected. Any legislation must be focused on the behavior associated with spyware, and that is fraud and deception. The malicious activities of purveyors of spyware must stop.

But technology is simply the tool that they use to create the problem. It is not the problem itself. For that reason, the NAI is strongly supportive of legislation that is technology neutral. And let me make one thing very clear. In a way that is very similar to the spam debate from 2 years ago, if we create legislative responses that focus on technology, the purveyors of spyware will simply move to newer, more surreptitious, and different technologies, leaving the companies that are legitimately using those technologies to bear the yolk of the compliance and the regulatory standards that have been placed upon them.

Other bills that we have seen introduced have gone far beyond the immediate concerns associated with fraudulent, deceptive spyware, and have proposed standards for online advertising that will be very harmful to the primary economic support for the vast quantities of free media online today. Make no mistake, the reason that Google can offer, perhaps, the most powerful search engine and research tool the world has ever seen, is because advertising supports their operation. The reason that Yahoo! and the *New York Times,* really every publisher in the world today, can offer free content online is because advertising supports those operations. Focusing in an excessive way on online advertising and spyware legislation calls into question, or may indeed threaten, some of those business models.

We must also be wary of spyware legislation that inappropriately includes online privacy standards. I think it would confuse the issue to discuss spyware at the same time that we discuss online privacy. And again, the NAI is an organization that has been dedicated to finding standards that are appropriate, and meaningful at the intersection of the online world and privacy. So, we are prepared and in fact are very open to and encouraged by discussions

of online privacy. But online privacy is a separate discussion from spyware, and we should handle them separately. Basically, the NAI feels that spyware legislation should focus carefully and precisely on fraudulent and deceptive practices.

Let me speak for a moment on another topic, and that is technological solutions to spyware. These solutions are a promising option, in fact, they are needed, and the NAI supports calls for consumers to have anti-spyware programs on their desktops. However, some anti-spyware technologies are inappropriately alarming consumers by flagging, and in some cases deleting, legitimate technologies. In one case, cookies. Cookies are not spyware, and any technological solution must be carefully tailored to recognize, and leave intact, legitimate tools used by companies legitimately engaged in the online economy.

The NAI feels strongly that solutions to spyware problems must be advanced. Federal preemptive legislation, aggressive enforcement of existing laws, accountable and transparent technological solutions and industry self-regulation can all work effectively toward eradicating fraudulent and deceptive practices of spyware.

Mr. Chairman, the members of the NAI pledge our support in this fight. Spyware is a complex problem, and our solutions must be thoughtful, robust, and comprehensive. I thank you for your time today, and I will be happy to take any questions.

[The prepared statement of Mr. Hughes follows:]

PREPARED STATEMENT OF J. TREVOR HUGHES, EXECUTIVE DIRECTOR, NETWORK ADVERTISING INITIATIVE

Mr. Chairman and members of the Committee, I want to thank you for inviting me to testify. My name is Trevor Hughes, and I am the Executive Director of the Network Advertising Initiative (NAI). The Network Advertising Initiative is a trade association representing companies concerned about issues of privacy, consumer protection, and online technologies. In this role, the NAI has taken a leadership position on issues of cookies, online advertising, spam, web beacons, the Platform for Privacy Preferences (P3P), and privacy legislation. The group has now turned its focus to the growing problem of spyware and the related concern of unintended consequences for legitimate technologies and business models.

The extent of the spyware problem has been reported extensively in the media. In many ways, spyware has become one of the most compelling consumer issues in the e-commerce and online world. Spyware can cause serious problems, and even cripple computer systems. There is ample anecdotal evidence of spyware substantially impairing the speed of consumers' computers. The fraudulent and deceptive nature of spyware has resulted in legitimate consumer outcry. Businesses also struggle under the onslaught of spyware. Employees' systems can be seriously compromised by spyware. This raises serious concerns about productivity, security, and corporate intellectual property. Untold hours of customer service support are being spent in response to spyware problems on consumer and employee desktops.

But the erosion of consumer trust in online activities and e-commerce is perhaps the most economically damaging effect of spyware. Billions of dollars have been spent in realizing the promise of e-commerce. Nearly every industry now uses online tools—including e-mail, instant messaging, internet telephony, and e-commerce generally—to transact business within companies and with customers. These investments are at peril if consumers distrust the very medium through which they are transacting business.

There have been numerous surveys and polls taken to determine whether the threat of spyware and other deceptive practices has influenced consumer confidence with the Internet. In August 2004, Greenfield Online conducted a poll regarding Internet user's concerns and perceptions regarding Internet security issues. According to the results, 80% are concerned about online identity theft, 72% would bank online for the first time if security was improved, and 90% of existing online bankers would utilize higher value services if there was better protection from identity

theft.[1] In a September 2004 Dell and IEF poll, almost 4 of every 10 people polled felt less secure using computers than a year earlier.[2] The results seem to show that consumers are becoming *weary* and *wary*.

When considered with the growing problems of phishing, ID theft, viruses, and general online fraud, the spyware problem exemplifies an increasing crisis in consumer confidence in the online channel. If spyware is allowed to proliferate, we will be left with a distinctly dystopian future in which the web is so polluted with fraud and deception as to be unusable by the public. In such a scenario, everyone loses.

Industry and public policy solutions to the spyware problem have been quick to arise. Clearly, companies engaged in the online economy have a strong incentive to eradicate spyware. But any legislative and technological solutions must be carefully crafted to ensure that we do not throw the proverbial baby out with the bath-water. We must be sure to protect benign technologies and legitimate business models as we pursue the purveyors of spyware.

We must also recognize the value of effective industry self regulation in the online economy. Legislative and technological responses frequently do not provide the fine tuning necessary to proscribe the boundaries of acceptable corporate practices online. There are many examples of strong self regulatory efforts in e-commerce that should be applauded and encouraged as a meaningful tool to address public policy concerns.

The Legislative Response

Over the past two years, many legislative proposals have been introduced in response to the spyware problem. Currently, there are at least 3 bills in Congress, and over 30 bills in the states. Four states have passed spyware legislation. It is possible, if not probable, that we will have over a dozen spyware laws at the state level by the close of this year. As these laws proliferate, the challenges for legitimate businesses to comply with the myriad of state standards increase significantly.

The members of the NAI feel strongly that Federal preemptive legislation is currently needed. We recognize, perhaps more than most other companies, the serious challenge presented by the growing gauntlet of state spyware laws. In the United States today, we have 4 spyware laws on the books (one is currently enjoined under a constitutional challenge) and over 30 bills proposed. If the trend towards state spyware legislation continues, we will end up with a crazy quilt of standards that makes compliance overly burdensome for legitimate business. In such a scenario, preemptive Federal legislation is necessary to set a common platform for the Nation.

But spyware legislation at the Federal level should not be passed only to create a common standard for the Nation. Rather, the primary focus of the legislation should be to address the dire threat posed by pernicious behavior online. Spyware is fundamentally an act of deception. And Federal spyware legislation should focus carefully on the fraudulent and deceptive behaviors associated with the problem. The NAI therefore strongly supports legislative efforts the target those acts associated with spyware that are fraudulent and deceptive in their very nature.

But how do we know what is fraudulent online? In the Spring of 2004, the Consumer Software Working Group (CSWG), a group formed under the leadership of Ari Schwartz from the Center for Democracy and Technology, recognized the growing concern over spyware and worked to compile a list of devious practices in downloaded applications (spyware). The CSWG categorized the practices into three areas, hijacking, surreptitious surveillance, and inhibiting termination. The CSWG list of devious practices is a valuable tool for identifying the fraudulent and deceptive practices that exist online. And the influence of the effort can be readily seen in Section 2 of H.R. 29, a leading spyware bill in the House of Representatives.

The NAI participated in the development of the CSWG devious practices list and applauds Mr. Schwartz and the CDT for their leadership on this important issue. Our members feel that Section 2 of H.R. 29 represents an important tool for combating fraud and deception in spyware.

Unfortunately, many of the legislative proposals currently under consideration go far beyond fraud and deception. Indeed, H.R. 29, while providing meaningful responses in Section 2 (dealing with deceptive practices) goes too far by proscribing many online advertising practices. The NAI does not support legislative standards that endeavor to place limits on the use of online advertising. Online advertising is the primary economic force that creates the enormous amount of free content we

---

[1] Survey Finds Identity Theft Negatively Impacting Consumer Use of the Internet, October 19, 2004, *http://biz.yahoo.com/prnews/041019/datu019_1.html*

[2] IED-Dell Survey conducted between September 17–19, 2004 by Ipsos-Public Affairs. Results also mentioned in the *Washington Post* article "Dell Joins Spyware Fight," October 18, 2004, *http://www.washingtonpost.com/wp-dyn/articles/A41629-2004Oct18.html*

enjoy online today. Proscribing online advertising will compromise that economic model, and may threaten the availability of free resources online.

Further, many legislative proposals confuse the spyware debate with online privacy. While there are definitely privacy violations that are occurring through spyware, a broad online privacy response that covers all online activities is not warranted. Online privacy should be considered separately from spyware.

Another approach that has been seen in response to spyware is to limit the technologies that the purveyors use to perpetrate their fraud. But this response is flawed. Spyware is not caused by technology. Indeed, in many cases the technology is irrelevant to the practice involved. If legislation were to limit a certain technology, the purveyors of spyware would simply move to, or develop, other technologies to continue their activities. Prohibiting or proscribing technologies is not good public policy.

A good example of a technology that has been implicated in the spyware debate is cookies. Put simply, a cookie is a mechanism that allows a website to recognize a particular computer as it visits that site. Cookies power a huge number of critical web functions today—preference management, shopping baskets, advertising, auditing and analytics all use cookies.

There have been privacy concerns related to the use of cookies, and these issues are valid and important. As a result, cookies have been thoroughly vetted through public policy channels. Cookies are not spyware. They have been thoroughly reviewed and managed through technology, regulation, and self regulation. Any further standards create very real threats to the reinvigorated online economy. E-commerce, online advertising, and free online content all pivot upon the use of cookies. Any legislation addressing spyware must make it clear that cookies are not spyware. A legislative approach that focuses on behavior (fraud and deception) and not technology will achieve this result.

Another issue that has arisen in the legislative debate over spyware is whether companies engaged in the technological responses to spyware (anti-spyware technologies) should be provided protections under the law. The members of the NAI feel strongly that *all* companies in the online world should be accountable for their actions. Providing a "good Samaritan" safe harbor for anti-spyware companies would remove the necessary checks and balances that encourage such companies to provide solutions that are carefully targeted at actual spyware. We therefore do not support such provisions.

Conclusion

The NAI feels strongly that spyware is a critical threat to e-commerce and online advertising. We applaud and support legislative efforts that are narrowly tailored to offer better tools to pursue fraud and deception. We stand together with advocates, consumers, and public policy leaders in demanding accountability for the nefarious actions of the purveyors of spyware.

However, much of the current discussion regarding spyware has inappropriately included limits on online advertising, privacy standards, and benign technologies such as cookies. Limits on online advertising and broad online privacy mandates are inappropriate in a spyware bill. And technological proscriptions may hinder the use of fundamental tools of e-commerce. Any restrictions on these technologies could have devastating consequences for the online economy.

The NAI therefore urges public policymakers to carefully draft any spyware standards to narrowly focus on fraud and deception. Legislation should be inherently technology-neutral and not impair the continued growth of the online advertising market.

But legislative solutions are not enough to solve the spyware problem. We need to have effective, and accountable, technologies to respond to the pollution on consumers' desktops. And industry self regulation must be supported to provide strong guidance for the legitimate actors in the online economy.

Mr. Chairman, on behalf of the members of the NAI, I pledge our efforts to continue to work on this issue and to support the important work of this committee in fighting spyware. Spyware is a complex problem, and our responses must be thoughtful, robust and comprehensive.

Thank you. I look forward to your questions.

Senator BURNS. Thank you very much. Now we have David Moll, who is Chief Executive Officer, Webroot Software, Incorporation, and thanks for coming this morning.

STATEMENT OF C. DAVID MOLL, CHIEF EXECUTIVE OFFICER, WEBROOT SOFTWARE, INC.

Mr. MOLL. Thank you, Senator Burns, and members of the Committee.

Senator BURNS. Pull the mike up. You've got a nice voice; we should have everybody hear it.

Mr. MOLL. Thank you, sir, I'm flattered.

Thank you for inviting me here today. My name is David Moll, and I am the CEO of Webroot Software in Boulder, Colorado. Webroot is a privately held company backed by some of the industry's leading venture capital firms, including Technology Crossover Ventures, Axel Partner, and Mayfield. I would like to ask that my complete written testimony be included in the record, and I will summarize for you here, the key points.

Founded in 1997, Webroot has created innovative privacy protection and performance solutions used by millions of computers users around the world. Our customers include Fortune 500 companies, Internet service providers, government agencies, higher education institutions, small businesses, and individuals. We are most well-known as the creators of a leading anti-spyware product, Spy Sweeper, released in 2003.

At the high level there are four primary ways that spyware represents a threat to us today: data security; online privacy; networking computer performance; and more broadly, Internet commerce. Data security is a key element. Whereas a primary risk of computer viruses has always been data corruption, spyware poses a very real threat to data security itself. Some of the most at-risk data today includes: national security information, including defense and homeland security; intellectual property and trade secrets; financial records; customer data; personal health information; and a wealth of other sensitive data such as passwords and account numbers. Instances where these risks have been realized are, in fact, numerous today and include shocking realities.

Hill Air Force Base in Utah, part of the Strategic Air Command, has identified and removed a substantial spyware infection, including keystroke loggers. The Oklahoma City, Kentucky Sheriff's office identified three PCs, seemingly a small example. However, each of these PCs had access to homeland security updates, prisoner transfer records and personnel files. Val Software, Incorporated, 3 years ago was penetrated by spyware and source code for their leading product that was then posted on the Internet, nearly crippling the company. A leading mutual fund company with more than 2,000 employees recently identified 8,000 high-risk pieces of spyware on their network in only 1 month of administering an anti-spyware solution. And finally, the payroll systems of the Bay City, Michigan school systems were found riddled with spyware, again, including keystroke loggers. These are just a few examples of a widespread problem that threatens data security across our country.

As it relates to online privacy, the privacy threat of spyware in this cyber age is the equivalent to trespassing in your home, much the way Senator Boxer suggested. Some of the types of information that can be collected by spyware programs without the informed consent of the computer owner, are your browsing habits, the sites you've visited, search terms you've used, advertisements you

clicked on, bookmarks or favorites that you've entered, contents you've downloaded, applications that you've used, entire e-mail or instant messaging conversations, user names, passwords, and certainly personal information such as social security numbers and credit card numbers.

During the first quarter of this year, one of our Nation's largest financial services companies determined that 100 percent of the fraud penetrated through their online banking portal was achieved through the use of spyware. As it relates to network and computer performance, at a minimum, it is a nuisance to have your computing resources used by programs you didn't knowingly install. Studies during the last year show that spyware consumes an inordinate amount of computing resource, and as spyware multiplies on a PC, the impact increases in a super linear fashion. With as few as three or four pieces of spyware on a single PC, and mind you, that the AOL study found as many as 90—the machine can become unusable—with its memory dominated by spyware processes, the hard drive used to cache advertisements, and the connection jammed with spyware/server communications. Not surprisingly, this leads to a larger economic impact in terms of the number of support calls caused by spyware—predominantly with Internet service providers and computer makers. Dell Computer determined—and this goes back to the 2003–2004 testimony that they gave to the FTC—one in five of the calls made to their consumer support line is driven by a spyware-related problem. This figure stands today. A leading global IT services firm has determined that spyware-related support calls to their internal help-desk makes up 70 percent of their support requests, costing that organization millions.

Finally, spyware poses a threat to Internet commerce itself. The increasing complexity and security concerns that arise from spyware, and the new uses of spyware in phishing and pharming attacks, have created a new level of user concern that threatens trust in the online economy. The threat has proven so dramatic that Citigroup recently entered into a partnership with Webroot to provide anti-spyware protection for their card holders and employees in defense of their customers and the folks who work for them. Based on recent Webroot research, there are more than 250,000 websites that leverage and exploit a security hole which allows spyware to contaminate a user's computer with no interaction from the user—a practice known as the drive-by download. Often this is affected from websites that leverage misspelled URLs, and including a recent example where Google.com suffered this very effect. This experience shakes the confidence of users, and deters e-commerce itself.

As shocking as some of the examples of spyware's victims may be, the pervasiveness is even more shocking. Webroot's survey of more than one million PCs last quarter, reveals that 88 percent of home computers, 64 percent if we exclude tracking cookies, and 87 percent of business computers, 55 percent without cookies, are infected with some form of spyware. I'll point to you the sample size here of more than a million PCs relative to that AOL study. We have a great deal of additional data about spyware that we have assembled in the Webroot State of Spyware report. I would like to

ask that a copy of this report be included, along with my testimony, in the hearing record and, members of the Committee, I think you've already received both hard and soft copies of this report.*

Senator BURNS. We have, and we will put that in the record.

Mr. MOLL. With the limited time that I have left, I'd like to move on to how we fight spyware. Individuals in the industry have been able to combat viruses successfully. Perpetrated by individuals, the defenses have been organized and well-funded. But, for the first time, we now fight an organized and well-funded threat. Spyware is part of a calculated business plan, or it's a tool that is used by criminals. In both cases, there are clear economic motives behind the proliferation of spyware. We believe that the advertising-inspired revenues here alone are in excess of $2 billion dollars annually, and the fraudulent side is rising as well. In order to effectively fight this problem, we need technical solutions, clear public policy and strong legal enforcement. In addition to existing law, which provides for complaints by the FTC and the attorneys general, we also anticipate benefits from legislation such as Senator Burns' bill. The bill provides additional clarity and focus on the problems that we are seeing, and we hope that it will induce additional attention from law enforcement agencies. Again, I thank you for inviting me here today, and I appreciate the opportunity to come and share with you some of what we have learned over the last few years. And, I welcome any questions.

[The prepared statement of Mr. Moll follows:]

PREPARED STATEMENT OF C. DAVID MOLL, CHIEF EXECUTIVE OFFICER, WEBROOT SOFTWARE, INC.

Chairman Stevens, Senator Inouye, and Committee members, thank you for inviting me to speak to you today. My name is David Moll and I am CEO of Webroot Software, headquartered in Boulder, Colorado. Webroot is a privately held company that is backed by some of the industry's leading venture capital firms, including Technology Crossover Ventures, Accel Partners and Mayfield.

Founded in 1997, Webroot has created innovative privacy, protection and performance solutions used by millions of computer users around the world. Our customers include Fortune 500 companies, Internet service providers, government agencies, higher education institutions, small businesses and individuals.

In 2002, our research team, which consisted of just two people, saw a growing pattern of undisclosed downloads that caused numerous problems for computer users. We joined a small band of early activists that began calling these kinds of programs spyware. We introduced a product called Spy Sweeper in February of 2003 to help our customers fight this newly identified problem. When first introduced, Spy Sweeper found around 200 various programs, and easily removed them all.

We have been running at breakneck speed to stay a step ahead of spyware ever since. Today, we are a company of 250 professionals focused on combating this problem. Our research team has grown to over 30 people, a good number of whom develop and maintain the automated tools we use to outpace the developments in spyware. Spy Sweeper, has also changed to adopt new weaponry to combat spyware that is increasingly hard to identify, and at times even harder to remove. This week we will introduce Spy Sweeper 4.0, our latest edition, with more than one-half million lines of software code. This our 14th major release of the product in a little more than two years.

The Effects of Spyware

Spyware and its ability to access a user's machine without informed consent for financial gain is an epidemic that threatens the viability of the Internet as a commerce, entertainment, communications and educational tool. Spyware programs can be used to facilitate the unauthorized use of computers for things like spam relay,

*The information referred to has been retained in Committee files.

and distributed denial of service attacks. Spyware programs can also lead to identity theft, and the theft of intellectual property, as well as data leaks, and the degradation of computer performance. Spyware is difficult to detect, and even more difficult (if not impossible) for the average user to completely remove manually.

At a high level, there are four primary ways that spyware presents a threat: data security; online privacy; network and computer performance; and Internet commerce broadly.

Data Security—Whereas a primary risk of computer viruses is data corruption, spyware poses very real threats to data security. Some of the most at risk data includes:

- national security including defense and homeland security;
- intellectual property and trade secrets;
- financial records;
- customer data;
- personal health information; and,
- other sensitive data such as passwords and account numbers.

Working with government entities and corporate customers over the past year, we have witnessed breaches involving each of these sensitive kinds of data. There are cases where spyware was used to infiltrate local law enforcement computers, trading and financial systems at financial institutions, payroll systems at Fortune 500 corporations, central databases for school systems, and entire municipal computer operations.

In these kinds of environments, even a very small number of system monitors or keyloggers puts highly-sensitive information at risk.

Privacy—When placed on a machine without the informed consent of the computer owner, spyware is the cyber-age equivalent of someone trespassing into your home. Some of the types of information collected by spyware programs without the knowledge of the computer owner are:

- browsing habits and sites visited;
- search terms used;
- advertisements clicked on;
- bookmarks and favorites;
- downloaded content;
- applications used;
- e-mail and instant message conversations;
- usernames and passwords; and
- personal information, such as social security numbers.

While few argue about the sanctity of personally identifiable information, we often hear the argument that collecting aggregated browser habits to provide more targeted advertising is not a privacy invasion. We disagree. In our view, it is wrong to download programs or data files without the informed consent of the computer owner for marketing purposes. Such marketing behavior begins the slippery slope of reasoning that leads to more egregious privacy violations by malicious spyware. Think about this in the offline environment. Would it be ok for a marketing firm to go into your home without your knowledge to look at the books on your shelves to decide what to market to you? Would it be ok if they did it to everyone and aggregated the data?

Computer and Network Performance—Spyware can seriously impact computer and network performance. At a minimum, it is an undesirable nuisance to have your computing resources used by programs you didn't install, and do not want. There is also a larger economic impact in terms of the number of support center calls caused by spyware. According to Dell Computer, one of every five customer support calls are related to spyware, adversely affecting the profitability of their consumer business.

In corporate environments, where many computers are centrally supported and managed, spyware can drive up the total cost of ownership in the IT system; a leading IT services firm estimates that spyware costs them millions annually in productivity and support costs, and constitutes as much as 70 percent of their internal help desk call volume.

In the worst cases, systems can crash from an overload of spyware programs, resulting in the loss of data and computer assets. This part of the spyware threat is too often overlooked or underestimated, yet productivity costs associated with spyware are far greater than spam.

Internet commerce—At a macro level, spyware also presents a threat to Internet commerce as a whole. The increasing complexity and security concerns that arise from spyware, and the new uses of spyware, such as phishing and pharming attacks, have created a new level of user concern.

Based on our recent research, there are more than 250,000 webpages that leverage a weakness we call an "exploit" which allows them to contaminate a user's computer with some form of spyware even when there is no interaction from the user—a practice known as a drive-by download. Quite often these sites hosting drive-by downloads operate using URLs that are commonly misspelled or mistyped alternatives to the URLs of popular sites. For example, just last week, Internet users planning to visit Google's site who inadvertently mistyped and entered *www.googkle.com* became the unwitting victims of drive-by downloads.

In the consumer world, spyware represents the same potential for fraud that internal spyware infections represent to corporations. For example a leading financial institution working with Webroot determined than 100 percent of the e-commerce fraud experienced by the bank in the past quarter was tied to spyware on end user machines. Spyware, keystroke loggers in particular, that can be installed from drive-by sites or via e-mails, have become new methods to those harvesting identities and defrauding consumers via the Internet.

As more people become aware of these numbers and understand the threat of spyware, we are concerned about an overall negative effect on consumer trust in the online economy.

The Growth of Spyware

Spyware has become pervasive. Webroot's survey of more than one million PCs in the last quarter reveals that 88 percent of home computers (64 percent if we exclude tracking cookies) and 87 percent of business computers (55 percent if we exclude tracking cookies) are infected with some form of spyware. The good news is that awareness is increasing, and more people are installing programs, like Webroot's Spy Sweeper, to prevent and contain spyware from impacting their system. The bad news is that the spyware purveyors are financially motivated, creative and resourceful. Therefore, we face a constant escalation in the amount of spyware we have to fight.

To give you an idea about the growth rate of spyware, Webroot identifies between 50 and 100 new pieces of spyware every week, and between 200 to 500 pieces of spyware that have "morphed" to avoid detection and removal. With the help of a spyware research system we call Phileas, which I will explain further later, Spy Sweeper currently detects about 88,000 spyware traces—individual files which make up a piece of spyware.

Understanding the growth of spyware requires more than just data about infection rates. It also requires that we understand the impetus behind propagating these programs. Spyware is not like a virus designed by a "script kiddie" who just wants to show off. Spyware is part of a calculated business plan, or a tool used by criminals. In both instances there are clear economic motives behind the proliferation of spyware.

In order to effectively fight this problem, it is essential that we have a clear picture of economic drivers, infection rates and trends. Recognizing this need, Webroot began work earlier this year to create a report that would encapsulate all of the key aspects of the issue. The result is the Webroot State of Spyware report which we issued this past week. This is a broad and detailed accounting of spyware today. We continue to compile this data, and we will issue updates to our report quarterly.

To ensure that you have all the information we assembled, I'd like to ask that a copy of the report be included in the hearing record as an appendix to my testimony.

Fighting Spyware

Until recently, the primary methods for fighting spyware were reactive. Anti-spyware companies concentrated on fixing an already infected machine. That alone presents a significant challenge, because in order for us to do our job correctly, we need to not only detect and quarantine the spyware programs, but we also need to ensure that we do not interfere with any legitimate files in the process.

Once we mastered the techniques to accomplish these two things, we worked to figure out a method that would not only cure spyware infections but also prevent them. Last year, we launched the Webroot Phileas Malware Crawler that I referenced earlier. Phileas is the anti-spyware industry's first automated spyware research system. Phileas deploys hundreds of automated programs—called bots—to crawl the Web searching for spyware. In less than an hour, a single Phileas bot completes the equivalent of 10 days of manual research by a trained person. With

the speed and scale of the Phileas system, we travel the Internet every day to find spyware before it attacks our customers. We complement systems like Phileas with "shields" built into the Spy Sweeper software which protect users' systems from the common behaviors of spyware, stopping the threat before it can take hold of a system.

Ultimately, we believe that it is best to fight technology with technology, and we remain committed to continuing to provide the very best commercially available technology solutions to fighting spyware. However, we also believe that there is a vital role for legislators, regulatory agencies and law enforcement to play in this fight.

As I stated earlier, there are economic motivations behind the growth of spyware. Some of the companies involved in the proliferation are considered legitimate U.S. based companies. The complaint filed by the FTC against Seismic, and the NY Attorney General's case against Intermix, demonstrate that there are cases that can be pursued under current law in U.S. Courts. We encourage enforcement agencies and attorneys general to deploy additional resources to join the fight against spyware. Companies need to understand that there will be costs associated with operating in ways that deceive and defraud consumers.

In addition to existing law, we at Webroot also anticipate benefits from legislation such as Senator Burns' bill, S. 687. The bill provides additional clarity and focus to the problems we are seeing, and I hope it will induce additional attention from enforcement agencies.

Conclusion

Again I thank you for inviting me here today. Spyware is something we have spent innumerable hours on over the last two years, and I appreciate the opportunity to come and share with you some of what we have learned. I welcome any questions you have for me.

I would also like to offer our assistance to all the members of the Committee. If, after today's hearing, any of you have additional questions we can answer or need information we can provide, please do not hesitate to contact us. Based on our attention to this problem, and our unique research capability, we are in a unique position to offer assistance, and welcome the opportunity to help in the formation of policy.

Senator BURNS. Thank you very much, Mr. Moll, and we have Ari Schwartz, he is Associate Director, Center for Democracy and Technology, and thank you for coming today, we work a lot with that group, and we appreciate you and are looking forward to your testimony.

STATEMENT OF ARI SCHWARTZ, ASSOCIATE DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY (CDT)

Mr. SCHWARTZ. Thank you, Senator Burns. members of the Committee, thank you for holding this hearing on spyware and inviting the Center for Democracy and Technology to testify today.

Since CDT last testified in front of this committee in the last Congress, spyware practices have gotten much worse. On a personal note, following this holiday season, I can count myself among the tens of thousands of technically astute consumers and computer professionals who have tried to help a family member fix their computer that has been plagued by spyware. This computer was so clogged that we decided it would be better just too simply reformat the hard drive.

On the brighter side, we have seen law enforcement start to take action against alleged spyware purveyors. Recently, the Attorney General of New York brought a case against a Los Angeles company called Intermix for deceptive and unfair practices in installing software. And in a case that received much less attention in October of last year, the FTC began its first public enforcement against a spyware company, a case against Seismic Entertainment. The FTC's lawsuit was based on a complaint filed earlier by CDT. In

that complaint, we specifically asked the FTC to investigate the affiliate relationships being exploited by companies to deflect responsibility and avoid accountability. The FTC has pursued financial records and e-mails in that case, and their investigation has now given us a clear picture of how current advertising practices on the web can go astray and lead to the installation of spyware.

There is little question that many consumers like the idea of free content in exchange for seeing advertisements, as long as it is their choice. But today we see too many cases of long affiliate chains where, at the end, companies are paying shady operators on a per installation basis. This pay per install model creates an incentive to cram extra software onto computers without regard to the wishes of the user.

The FTC's discovery in the Seismic case shows through e-mails that Seismic worked with various players to take advantage of the current system. CDT has tried to follow the resulting trail. In our testimony, we have a graphic detailing what we know about this case to help serve as an example. We provided the Senators with a one page blow up copy of this graphic. If you are confused by this trail, you are not alone. The complex mess of advertisers, adware companies, ad networks, distributors, affiliates and websites is enough to make even a seasoned analyst's head spin.

To clarify a little, Seismic would use fake public service announcements to infect the computer through a hole in the browser. In one e-mail message, the head of Seismic proudly proclaimed, "I figured out a way to install an executable file without any user interaction. This is the time to make the money while we can."

Later, he explained to one of his partners that they worked on weekends because it takes longer for the ad networks to shut them down. The e-mails also show a pattern that they would go back to the same ad networks time and time again. Adware networks should have caught onto this, but unfortunately based on the e-mail available, only a couple seemed to care about this clear pattern of abuse.

Once Seismic had gained a foothold in the user's computer through the infected banner, it would install the dozens of programs, including those from large companies, like 180 Solutions. 180 Solutions software then delivered popups onto the user's computer. As the *LA Times* detailed in a piece at the beginning of this week that Senator Wyden also mentioned, many of the mainstream companies have no idea that their ads are showing up on 180 Solutions software, let alone through nefarious installations like this one.

CDT sees four major areas where action is necessary to combat spyware, and stem the disturbing trend toward a loss of control and transparency for Internet users. First, enforcement of existing law. Second, better consumer education, and industry self-regulation. Third, improved anti-spyware technologies, and fourth, baseline Internet privacy legislation. Carefully targeted spyware-specific legislation may also have a role to play, especially as it relates to improved enforcement, and building incentives for positive action.

However, we hope that such legislation is not seen as an alternative for baseline standards for online privacy. The absence of pri-

vacy rules has created a kind of "wild west" atmosphere that we've seen in too many cases. Privacy legislation can put in place a framework for addressing issues like spyware before they've reached epidemic proportions, rather than only legislating reactively.

CDT believes that we can address this problem, but it will take a sustained commitment from technology companies, the advertising community, and law enforcement, to stem these bad practices. I look forward to your questions.

[The prepared statement of Mr. Schwartz follows:]

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

Chairman Stevens and Ranking Member Inouye, thank you for holding this hearing on spyware, an issue of serious concern for consumers and businesses alike. CDT is honored to have the opportunity to speak with you today about spyware and the businesses behind it.

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

As an organization dedicated both to protecting consumer privacy and to preserving openness and innovation online, CDT has sought to promote responses to the spyware epidemic that provide meaningful protection for users while avoiding overly burdensome regulation of online commerce, software development, and business models. Last year we testified before the Subcommittee on Communications on the issue of spyware, attempting to define the problem and suggest the range of responses required to address it. Since that time, we have worked closely with members of industry, other consumer advocates, legislators, and others in government to more fully understand and begin to address this complex and important issue. We look forward to continuing this effort with members of the Committee and others in Congress and elsewhere.

> *"I figured out a way to install an exe without any user interaction. This is the time to make the $$$ while we can."*[2]

These two sentences, the body of an e-mail uncovered by the FTC in its recent case against a network of spyware purveyors, provide a rare window into the heart of the spyware problem. The alarming spread of deceptive download practices and stealthy, nefarious applications is a major threat to Internet users and to the long-term health of the open and decentralized Internet. It is a threat that exists because of the massive quantities of money to be made propagating these applications. Sanford Wallace, the spyware purveyor who wrote the lines above, brought in at least

---

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

[2] Federal Trade Comm'n. Mem. in Support of Leave to Name Additional Def.'s. and File First Am. Compl., Att. A, *Federal Trade Comm'n* v. *Seismic Entertainment Productions, Inc., et al,* 04–377 (D. N.H.) [hereinafter FTC Mem.]

$1.5 million from browser hijacking and deceptive software downloads in 2003 and 2004.[3]

As a whole, spyware and its close cousin adware are a multimillion dollar industry.[4] Deceptive and often clearly illegal software download practices are a regular part of the business of many American companies operating in online commerce. These practices are funded and incentivized through poorly policed download commission programs, programs that, in turn, are funded by large, mainstream advertisers. The entire process is sustained through a nearly impenetrable web of affiliate relationships that is used to deflect accountability and frustrate law enforcement. Many of the companies involved, particularly the advertisers, have no idea what is going on.[5]

CDT sees four major areas where action is necessary to combat spyware and stem the disturbing trend toward a loss of control and transparency for Internet users: (1) enforcement of existing law; (2) better consumer education and industry self-regulation; (3) improved anti-spyware technologies; and (4) baseline Internet privacy legislation.

Carefully targeted, spyware specific legislation may also have a role to play. However, we hope that such legislation is not seen as an alternative for baseline standards for online privacy, now that many companies have expressed their support for such a goal. Privacy legislation would provide businesses with guidance about their responsibilities as they deploy new technologies and business models that involve the collection of information. It would put in place a framework for addressing issues like spyware before they reach epidemic proportions, rather than legislating reactively. Finally, privacy assurances in law would give consumers some measure of confidence that their privacy is protected as companies roll out new ventures.

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

1. What is Spyware?

No precise definition of spyware exists. The term has been applied to software ranging from "keystroke loggers" that capture every key typed on a particular computer; to advertising applications that track users' web browsing; to programs that hijack users' system settings. Much attention has been focused on the surveillance dimension of the spyware issue, though the problem is in fact much broader than that.[6]

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

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

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

Each of these behaviors was specifically documented by CDT or reported to us by individual users frustrated by their inability to use their own systems. Although no single behavior of this kind defines "spyware," together these practices characterize

---

[3] The FTC found that Wallace received nearly $700,000 from OptInTrade and over $900,000 from Mail Wiper, Inc. and Spy Deleter, Inc. (FTC Mem. at 7, 10).

[4] One recent article cites estimates between $500 milliion and $2 billion. We believe these estimates are based on research by Esther Dyson and Webroot, respectively. *See* Joseph Menn, *Big Firms' Ad Bucks Also Fund Spyware, L.A. Times,* May 9, 2005.

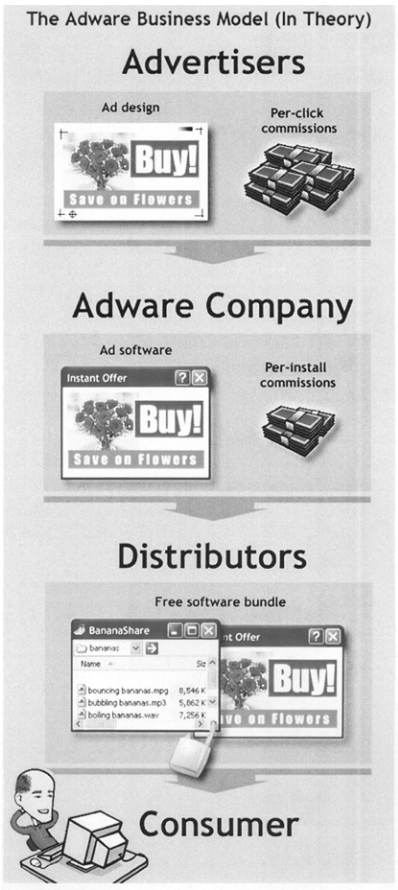
[5] *See* Menn, *Big Firms' Ad Bucks Also Fund Spyware*.

[6] Some argue that the term "spyware" should be used exclusively for software that records and transmits consumer information, whereas the broader category of nefarious applications that we use the term to describe should instead be called "malware." Regardless, the problem consumers face is the same: a flood of unwanted applications, some of which collect information and some of which exhibit other objectionable behaviors.

the transparency and control problems common to applications that warrant the "spyware" moniker.

2. The Spyware Business: Theory and Practice

While it is exceptionally difficult to obtain precise data on the prevalence of the spyware problem, the best study done to date, conducted by AOL and the Nation CyberSecurity Alliance, found that 80% of broadband and dial-up users had adware or spyware programs running on their computers.[7] Based on consumer complaints we have received[8] and our own research, CDT believes that the prevalence of egregious spyware and clearly unlawful violations has increased dramatically. Of particular concern is the use of security holes in web browsers to silently force software onto users' computers. Many Internet users may simply be turning off the Internet in response to these threats.[9]



[7] *http://www.staysafeonline.info/news/safety*__study__v04.pdf

[8] When CDT first became involved in the spyware issue, we launched a "Campaign Against Spyware," calling on Internet users to send us their experiences with these invasive applications, as mentioned in footnote 1 above. We indicated that we would investigate the complaints received and, where we believed appropriate, file complaints with the FTC. In our appearance before the Communications Subcommittee, we testified regarding the dramatic response to our campaign. In the nine months since our last appearance, CDT has continued to receive complaints through our online submission form. Among what are now hundreds of complaints, a total which continues to grow daily, are regular reports of new spyware programs arising. *See http://www.cdt.org/action/spyware*

[9] *See, e.g.* Joseph Menn, *No More Internet for Them, L.A. Times,* Jan., 14, 2005, at A1.

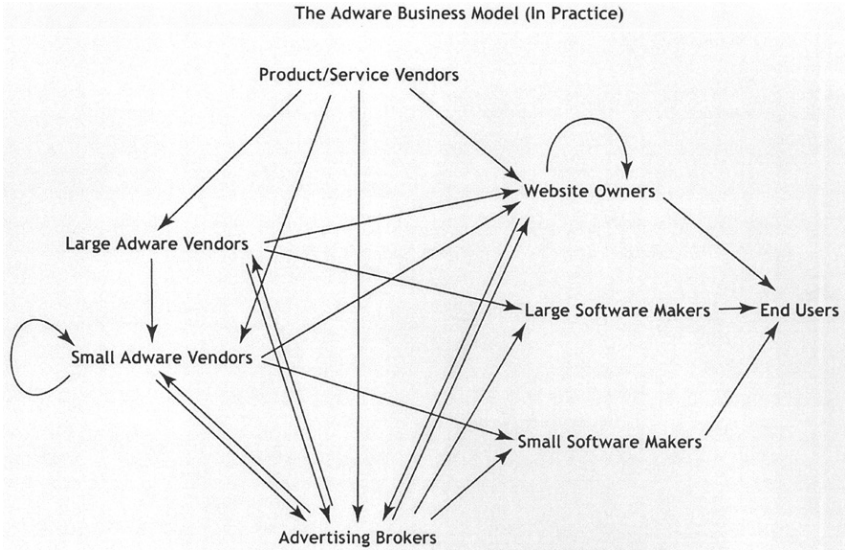
At the heart of this problem is the affiliate-marketing business model by which many advertising applications (adware) are spread. We want to take the opportunity in our testimony today to highlight and explain this issue, which has not been given sufficient attention to date.

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

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

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

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



The consequence of ubiquitous affiliate arrangements is that when an advertisement ends up on a user's computer, it will be many steps removed from the advertiser who paid for it. Similarly, the installation of the adware that is causing the ad may have been performed by a company that is far down the chain from the company that actually programmed the software. The existence of this complex network of intermediaries exacerbates the spyware problem in several ways. For example:

- *Industry Responsibility*—Adware companies, advertising brokers, and others all often disclaim responsibility for deceptive spyware practices, while encouraging these behaviors through their affiliate schemes and doing little to police the net-

works of affiliates acting on their behalf. Advertisers, too, should be pushed to take greater responsibility for the companies they advertise with.[10]

- *Enforcement*—Complex webs of affiliate relationships obstruct law enforcement efforts to find the parties responsible for spyware outbreaks. The complexity of these cases puts an extreme strain on enforcement agencies, which struggle to tackle the problem with limited resources.
- *Consumer Notice*—Adware companies and their affiliates have been reluctant to clearly disclose their relationships in a way that is transparent to consumers. CDT has suggested specific ways that adware companies could improve branding of their ads to help consumers understand bundling arrangements.[11] For the most part, companies have resisted these changes.[12] Efforts to bring transparency to the full chain of affiliate and distribution arrangements have met with even greater opposition.

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

3. A Real World Example of the Spyware Business

In October of last year, the FTC began the first public enforcement action against purveyors of spyware, a case against Sanford Wallace and his New Hampshire company Seismic Entertainment.[13] The FTC's lawsuit was based on a complaint filed earlier by CDT. In that complaint, we specifically asked the Commission to investigate the affiliate relationships between the parties involved. We highlighted the problem of affiliate relationship being "exploited by companies to deflect responsibility and avoid accountability."[14] The FTC pursued financial records and e-mails in the case, and its investigation has now given us a clear picture of how the adware business model can go very wrong.

The facts in the Seismic case, from the consumer's perspective, were as follows: An Internet user browsing the web would go to any of a variety of online sports, gaming, or other sites that carried banner advertising. The user would see an innocuous seeming banner advertisement, often a public service ad. Unbeknownst to him, however, the banner contained code that would launch pop-ups and change his homepage. The pop-ups and homepage hijacking were triggered when the banner was loaded, whether or not the user clicked on it. The next time the user opened his browser, he would be directed to a full page advertisement for anti-spyware software. This offer to remove unwanted programs and pop-ups (for $30) would appear even as adware programs were being silently installed on the user's computer. These programs would cause a barrage of pop-ups whenever the user surfed the web, they would add a toolbar and new "favorites" to his browser, and they would deposit icons on his desktop.

---

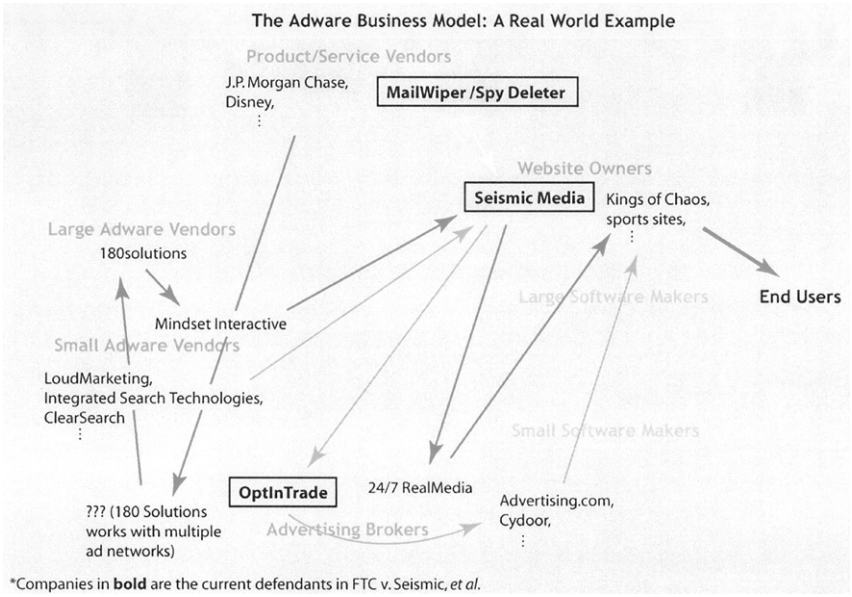
[10] Examples of steps in this direction include public policies by Dell, Major League Baseball, and Verizon setting standards for what software companies they will advertise with. Similarly, Google has drafted a specific public policy on what other applications it will bundle its utilities with. *See http://www.google.com/corporate/software_principles.html.*

[11] Center for Democracy & Technology, Comments to FTC Workshop on File-Sharing Workshop, Nov. 15, 2004.

[12] WhenU, one of the large adware companies, recently introduced co-branding for some ads. WhenU is currently the only adware company to co-brand.

[13] *Federal Trade Comm'n* v. *Seismic Entertainment Productions, Inc., et al,* 04–377 (D. N.H.)

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



CDT traced the nefarious banner ads that triggered this whole chain of events back to Seismic Entertainment. Based on CDT's research and the FTC's discovery, we now have a partial picture of what was happening behind the scenes in the case. Our current understanding of the network of affiliate arrangements is illustrated above—a map that would be confusing even to many of the companies in it.

A. Placing the Spyware-Spreading Ads

Once Seismic developed code to change users homepages and stealthily install programs, the company had to find a way to place this code in websites viewed by large numbers of Internet users. To do this, Seismic incorporated the code into innocuous seeming banner ads, often public interest ads as described above. Seismic would then pay large advertising brokers to incorporate the ads into their rotations. In the cases we know of, this was accomplished through a bait and switch: the ad brokers would be shown one set of normal, uninfected ads. Then at the last minute (and often over the weekend in order to make detection more difficult) the benign ad would be switched with one that looked superficially identical, but contained the infectious spyware code. In this way, the infected ads would appear on sites that had agreements with the ad network, whether sports sites, gaming sites, or other popular online destinations that used ad revenue to support their services.

Often Seismic would use a "front man" to further obfuscate the situation. We know that soon after Seismic figured out how to silently install applications, the company contacted a prospective partner, OptInTrade:

> From: <MasterWebFanClub@aol.com>
> To: jared@optintrade.com
> Date: Sat, Mar–6–2004 4:51 PM
> Subject: I DID IT
>
> I figured out a way to install an exe without any user interaction. This is the time to make the $$$ while we can.

Seismic and OptInTrade agreed that OptInTrade would deal with the advertising networks. When the networks discovered that the benign advertisements they had approved had been replaced by malicious versions, OptInTrade would feign ignorance and lay the blame on its upstream affiliate. In exchange for playing this role, OptInTrade would receive a portion of Seismic's revenues from the scheme. One exchange between Seismic and OptInTrade, laying out this strategy, was uncovered by the FTC:

> From: <MasterWebFanClub@aol.com>
> To: jared@optintrade.com
> Date: Fri, Nov–28–2003 12:37 PM

> Subject: strategy
>
> I do my sneaky shit with adv.com today through Sunday—everyone's off anyway. . . . You then send an e-mail to your contact early Monday AM saying the advertiser was unethical and pulled a switch and you are no longer doing business with them. . . . Then we stop buying adv.com through you in any way.

We know from other e-mails that this strategy was in fact carried out. One ad network, a company called CyDoor, complained to OptInTrade about the spyware infected ads that it had placed:

> From: Bob Regular [mailto:bob@cydoor.com]
> Sent: Sunday, December 21, 2003 12:45 PM
> To: "Jared Lansky"
> Subject: Please Terminate OptinTrade Online Pharmacy—Violated Agreementt
>
> [. . .] traffic just informed me your launching pops from your banners that force change in you homepage and stall your computer [. . .] I simply do not understand how this could happen again.

In response, OptInTrade told CyDoor that the ads were "from a new advertiser" and that they had "no idea how this is happening:"

> From: Jared Lansky [mailto:jared@optintrade.com]
> Sent: Sunday, December 21, 2003 9:25 PM
> To: Bob Regular
> Subject: RE: Please Terminate OptinTrade Online Pharmacy—Violated Agreement
>
> Hi Bob—The pharmacy campaign was a new advertiser with a new code set. When tested it didn't launch pops or change my homepage so I approved it to run with you. I have no idea how this is happening [. . .]

In fact, OptInTrade knew exactly what was going on.

B. Sources of Funding: Adware Companies and Advertisers

Seismic's infected banners made the company a surprising amount of money. Seismic's revenues came largely from per-install commissions paid by the adware companies. These companies pay a set amount every time one of their affiliates installs their program. Seismic would install the adware applications through its stealth process, and then collect the commissions—hundreds of thousands of dollars worth, based on documents uncovered by the FTC.

We know from records uncovered by the FTC and from CDT's own research that the long list of companies involved in the distribution chain for the adware applications installed by Seismic included LoudMarketing,[15] Integrated Search Technologies, ClearSearch, Mindset Interactive, and 180 Solutions. We do not yet know the exact nature of these companies' involvement or their level of knowledge about the scheme.

We do know, however, that in at least one case, the support for the adware came originally from major online companies. 180 Solutions is paid by large travel sites, online merchants, and others to serve advertisements for their services.[16] In this case, a portion of those revenues were passed on to a 180 Solutions distributor, Mindset Interactive. That company, either directly or through other affiliates, paid Seismic for installations—installations that Seismic would get through its devious infected banner ads.

In this way, large legitimate companies came to fund clearly illegal spyware distribution practices. Because of the lengthy and complex chain of affiliates involved, they almost certainly did so unintentionally and unknowingly.

4. Combating Spyware

Combating spyware—and the affiliate problems behind it—requires a combination of aggressive law enforcement, private efforts, and legislation. Significant progress has already been made since the spyware issue first began to receive national attention over a year ago, but much ground still remains.

---

[15] LoudMarketing, a Canadian company also known as LoudCash, CDT Inc. (no relation to the Center for Democracy and Technology), and a host of other names, was recently purchased by 180 Solutions.

[16] The two examples used in our chart, J.P. Morgan Chase and Disney, are taken from Menn, *Big Firms' Ad Bucks Also Fund Spyware.* We do not know conclusively (and it would be nearly impossible to determine) whether these two companies were advertising with 180 Solutions during the precise time that 180 Solutions' products were being covertly installed through Seismic. Rather, they are intended to serve primarily as examples of the many large, mainstream companies that advertise through adware.

A. Law enforcement

Much spyware is currently covered by Section 5 of the FTC Act, banning unfair and deceptive trade practices, as well as by the Computer Fraud and Abuse Act or the Electronic Communications Privacy Act. Spyware purveyors are also likely violating a variety of state statutes.

The FTC's case against Seismic *et al.,* described in detail above, represents an admirable first step in the enforcement effort. We applaud the Commission for its work on the case, which has led to an injunction against further exploitative practices by Seismic, and the extensive discovery regarding Seismic's affiliates that we have described. We hope and expect that the Commission will continue to pursue the web of affiliates in this case and to add defendants as appropriate.

In addition, the Attorney General of New York recently brought a case against an L.A.-based company, Intermix Media, alleging that the company had installed a wide range of advertising software on home computers without giving consumers proper notice.[17] CDT applauds the Attorney General's action, as state enforcement is badly needed in this area to supplement Federal cases.

Indeed, both the FTC and other national and state level law enforcement agencies must actively pursue further cases. Both the number and frequency of cases must be dramatically increased if law enforcement is to provide a significant deterrent to purveyors of spyware and to serve as a wake-up call to the many upstream companies that are currently partnering with and funding these bad actors.

B. Self Regulation and Consumer Education

Consumer education and sound best practices for downloadable software are sorely needed. Consumer protection bodies have a crucial role to play in educating consumers.

In addition, CDT has been contacting advertisers that are the root source of funding for spyware. We are encouraging advertisers to take a hard look at their policies and affiliate agreements. Companies should be actively creating and endorsing quality control policies for advertising delivery, and they should refuse to partner with adware companies until those companies clean up their acts, ensuring that all the users who get their ads have consented to receive them.

C. Anti-Spyware Technologies

Spyware blocking and removal tools, and other innovative forms of anti-spyware technology, are a crucial component of consumers' spyware protection.

In order to help advance anti-spyware technology, CDT convened a meeting in March with industry leaders and others to discuss issues facing the anti-spyware industry, including those that impact the industry's ability to ensure user control and empowerment. The participants shared their commitment to ensuring that users maintain control over what is on their computers. The participants also agreed to work together to better educate consumers about available tools and to develop shared terminology and approaches. Participants included: Aluria; AOL; Computer Associates; EarthLink; HP; Lavasoft; McAfee Inc.; Microsoft; Safer-Networking Ltd.; Symantec; Trend Micro; Webroot Software; Yahoo! Inc.; Samuelson Law, Technology & Public Policy Clinic at Boalt Hall School of Law, UC Berkeley; Business Software Alliance; and the Cyber Security Industry Alliance.

The group plans to meet again and will invite other consumer groups to join the effort as the members create public working drafts that address the group's chief goal of helping users and organizations take back control of their computers.

D. Legislation

CDT has been supportive of legislative efforts against spyware, yet we also want to make clear that there is only so much that new legislation can do. We endorse the idea of calling specific attention to the worst types of deceptive software practices online as most of the spyware bills do. Enforcement will be crucial to any legislative effort. Therefore, we are strongly supportive of including powers for state attorneys general. In addition, any legislation must take care to ensure that the use of complex affiliate relationships, as outlined above, will not enable responsible parties to avoid liability.

Senator Conrad Burns (R–MT), Senator Barbara Boxer (D–CA) and Senator Ron Wyden (D–OR), should be commended for their leadership to accomplish these goals through the new version of the SPYBLOCK Act (S.687). It marks a substantial step forward in addressing many of the concerns of consumer groups and companies.

CDT also remains firmly committed to the idea that a long-term solution to spyware and other similar issues requires baseline online privacy legislation. Many

[17] *See http://www.oag.state.ny.us/press/2005/apr/apr28a__05.html.*

of the issues raised by spyware may be easier to deal with in this context. This approach will also help us head off similar epidemics in the future, rather than reacting to them legislatively only after the fact.

Indeed, CDT hopes that the current effort on spyware can provide a jumping off point for efforts to craft baseline standards for online privacy now that many companies have expressed their support for such a goal. Otherwise, we will simply be back in this same place when we confront the next privacy-invasive technology.

5. Conclusion

Users should have control over what programs are installed on their computers and over how their Internet connections are used. They should be able to rely on a predictable web-browsing experience and the ability to determine what programs are on their computer and to keep out those they do not want. The widespread proliferation of invasive software applications takes away this control.

Addressing the spyware problem at its root requires understanding and responding to the problem of affiliate marketing. Industry self-policing and aggressive law enforcement by Federal and State authorities can help combat this phenomenon. Continued consumer education, and improved anti-spyware tools are also key to giving consumers control back over their online experiences. New laws, if carefully crafted, may also have a role to play.

The potential of the Internet will be substantially harmed if the current spyware epidemic continues. We look forward to continued work with this Committee to find creative ways to address this problem through law, technology, public education and industry initiatives.

Senator BURNS. Thank you very much, Mr. Schwartz. I will start the questioning here, and I will start with you because you mentioned this thing of the need of more privacy legislation. Are you saying that we should go back and reexamine the old Privacy Act and make some changes now because technology has changed?

Mr. SCHWARTZ. Yes, that's exactly what I'm saying. We need to take a look; you know we've had issues of cookies come before this committee, 6 or 7 years ago. Spam has come up again and again; we've had this discussion, as Senator Nelson said, with the data brokers and some of those issues as they reach online. We have the issue of RFID chips, and all of these come up again and again, and we don't have the basic framework online to deal with these issues and how they relate to the Internet. And that causes us to have to go and reexamine these problems every time, reexamine notice, reexamine consent, reexamine choices.

Some companies are beginning to come around to the idea that today, they're beginning to come around to the idea that privacy legislation could actually help in the future if it's done right. And it's going to be hard to do it right, and we see that, and we're not necessarily saying that it should be done only to go after spyware. We think it should be a bigger discussion, but we need to reinvigorate that debate again.

Senator BURNS. Mr. Moll, how would you react to that because you are in that business, and it seems to me there's a very fine line here that makes policymakers, and especially when you set anything into law, are we going to have to change as technology changes, but how do we deal with that?

Mr. MOLL. I think there are some principles that are timeless, and I point back to the Fair Information Practice principles that the FTC rolled out in the 1990s as still being, in fact, timeless and highly relevant. I do think that as technology continues to morph, (and I'll point out that today we are talking about PCs, we are not talking about PDAs and cell phones, and spyware and privacy threats will ultimately govern those devices as well), there needs

to be a constant vigilance around how this is going to apply to new technologies.

Senator BURNS. Mr. Hughes, advertising is very, very important to all of us. That's what maintains our free over-the-air television and radio and it also provides the engine that allows us to be on many of our Internet services for a very, very low cost. In your testimony you are saying move with caution. Have you provided this committee, and I know we have been working with you a little bit on this, that's a fine line also.

Mr. HUGHES. It's mostly definitely a fine line. But actually, I would say that we should not move with caution, we should actually move with purpose and actually move aggressively. We have had the opportunity to review Senator Allen's proposal, we think that it has many of the components that we feel are important and right.

What we have seen in the spam debate is that strong enforcement has an incredible deterrent effect in the market place. I frequently say that we will solve the spam problem and I think we'll solve the spyware problem when we see more purveyors of this fraud and deception coming out of Federal courthouses with raincoats over their heads, being led away. I think that that deterrent effect is absolutely necessary.

So legislation that focuses on fraud and deception provides preemptive standards so that we have a national level, a national platform for legitimate business to comply with and work from, and strong enforcement tools, I think would be something that we need immediately.

Senator BURNS. Can we stay ahead of it?

Mr. HUGHES. I think we are too far behind it right now to get ahead of it. I can foresee a future, sort of between those two dystopian visions that I described in which we do have control over it, and let me again refer back to the spam debate. Two years ago many were ready to throw their hands in the air and say that e-mail was a lost cause. That the channel of e-mail had indeed become so polluted. And, in fact, legitimate businesses were seeing e-mail filtering for spam filtering, some of the Bazian filters, content word filters, flagging messages that were entirely innocent, in fact, legitimate, and in some cases, absolutely necessary that the recipient received them. We were in a bad state, but we got a great combination of the CAN–SPAM Act, strong technological responses including e-mail authentication which is moving forward aggressively now, and AOL recently had given us some very good news, that we may be turning the corner in the spam fight. So, I most definitely can foresee a future when we turn the corner on the spyware fight.

Senator BURNS. Government can do some, we as policymakers can pass a law, but I think it takes, and you tell me if I'm wrong, it takes all the industries that all three of you represent, working together because there's no way we can be agile enough—the only thing we can set up is the framework—but I think most of the responsibility falls on you folks who represent the different ends of industry.

Mr. HUGHES. Senator, if I could, we actually scheduled our meeting first, but tomorrow we have almost two hundred members of this industry, including Mr. Schwartz and representatives from Mr.

Moll's company, meeting in New York City to do exactly that. To move the discussion in the dialogue forward. So I am looking forward to hosting 200 of our colleagues who care desperately about this issue tomorrow in New York City.

Senator BURNS. You should have met in Billings, Montana, but other than that, that's fine. Mr. Allen?

Senator ALLEN. Thank you, Mr. Chairman. I will ask all the witnesses here these questions. Do you all believe that the FTC currently has the authority to bring action against those who are purveying these deceptive and fraudulent means of surreptitiously downloading software on consumers' computers? Do you all think they have the authority?

Mr. SCHWARTZ. Yes, they have the authority and they have tools to do it. We're concerned about, as you said, some of the disgorgement issues and some of the—being able to go down the chain a little bit further—and whether they have the resources to bring those cases.

Senator ALLEN. Do you all agree?

Mr. MOLL. Senator, I would add one element, and that is that the Internet, and the notion of click-through licenses create new elements that I don't think were embodied in many of the laws, both at the State and Federal level that govern fair advertising. So in as much as they may have authority, I think there may be questions of application.

Senator ALLEN. Let me understand that again?

Mr. MOLL. Well, I think that there are elements today contained in end user license agreements that suggest that the user has given permission to install software that plays ads. And I think that the notion of that click-through license is at the heart of some of the adware debate that will be part of the spyware debate we are going to have to facilitate here.

Senator ALLEN. Would that not be a fraudulent and deceptive practice?

Mr. MOLL. That, I think, is up for question, and my belief is absolutely. I think there are others who disagree.

Senator ALLEN. Mr. Hughes?

Mr. HUGHES. Senator, I would concur, I think the FTC Act provides great tools for the FTC to go after the purveyors of spyware. There are a couple of components that I think would be helpful, disgorgement, clearly, but also preemption. We work in a medium, the web that is fundamentally borderless, and for a legitimate business to try and draw lines around state boundaries and comply with differing state standards is a real challenge. I think the web really lends itself to a jurisdiction of the highest level and therefore we are supportive of Federal preemptive legislation.

Senator ALLEN. I call it a national standard, and the reason is that we do have a number of states acting, and you can understand why states are acting, but this is a national—it's indeed an international problem. And the approach I think we are taking, my bill as well as Senator Burns' bill, different than the house version is that we do allow, obviously, the FTC and Federal authorities to prosecute these criminal activities. In the event that the states' attorneys general want to be involved, they also can, and both of us have that whereas the House version does not.

The impetus, all of you all agree that there's Federal jurisdiction, Federal authority. Do you agree that the main problem, problems, are one, they don't have the resources to investigate and prosecute—and so in our measure, the measure that Senator Smith and Ensign and I have introduced adds $10 million in funding, the disgorgement aspects of getting after ill-gotten gains. Ultimately, I think one way to fund it is to treat them somewhat similar to what I have done in the past with drug dealers, if they have ill-gotten gains off those assets, the jewelry, art object, yachts, cars, and give it to law enforcement for them to make undercover drug buys, pay informants, and so forth. It's like catching a shark and cutting it up for bait to catch more sharks, as opposed to the taxpayers. Those are the main approaches, as well, I think, the need for those in the industry to find ways to educate the public, consumers at home or in businesses how there are technologies to block spyware, just as was done with spam more recently.

Do you think that adding $10 million to their enforcement efforts, as well as discouragement would have that salutary effect of deterring, as well as, do you all agree that there ought to be a national standard here, as opposed to—I see them all nodding yes for the record for this court reporter, do any of you disagree?

Mr. SCHWARTZ. Senator, can I?

Senator ALLEN. Yes.

Mr. SCHWARTZ. One issue that you just raised there about some of the funding issues, I think it's important to realize that you can look at that chart that we put together of the Seismic case, and mapping that case out takes a lot of resources just to get to the point of finding the chain and tracking down the chain. They need the kind of forensic resources at the FTC and at the state level, actually, to be able to go after these bad guys all the way down the chain. That's something we don't really have today. In the Seismic case, we were able to spend our own money and work with others on the net to try and do the forensic work that put out the basic outline of the chain, so that we could turn it over to the FTC, and then they could pick it up from there.

The Intermix Case is a more direct case than we usually see, the one that Attorney General Spitzer's bringing, so we're talking, to get really to the root of the problem it's going to take more resources and kind of new skills to some of these law enforcement agencies that they perhaps don't have today.

Senator ALLEN. That's good advice. I'm not sure if $10 million dollars is all that it takes, but it's a substantial amount of money. It's not as if this is an easy effort that people instinctively know how to investigate.

Let me finish in the last minute here. On the issue of a national standard would you all agree in the need for preemption that if we don't have that, you could have 50 different state standards for this, as well as the global marketplace and actually, then have such a confusing situation, it would actually harm the ability of us to prosecute nationally and internationally?

Mr. MOLL. Senator, if I may, I think you've hit on a very good point there. And to the point that we want to defend the advertising industry that is legitimate, I think that is the most key element right now. With the current trajectory of state laws that vary

in their application and definition as widely as they do (and I'll point out, there are 27 states that have a bill either passed, or somewhere in process) this becomes untenable for people to thwart the problem, as we do in the anti-spyware industry and for people in the advertising business, for advertisers themselves.

Further, I think that on the international level, the EU is currently in consideration of legislation which will obviously provide for some consistency there. So I think that we'd be in good stead to follow suit and have a national standard.

Senator ALLEN. That's good to know, I will be holding a hearing this afternoon, Mr. Chairman, EU, European Commission and U.S. technology issues, and this would be a good one. Let me point out our measure that we have introduced has the toughest penalties than any state has. I wanted to make it so we are not somehow having lower penalties. We have tougher penalties than any other state as well as allowing treble penalties, and damages as well.

Senator BURNS. Senator Nelson?

Senator NELSON. Thank you, Mr. Chairman. If we don't put an end to spyware, spam, and identity theft, people are going to be gun shy about using their computer. I couldn't help but think of a thorny issue that we have coming before us by the end of this year which is the reenactment of U.S.A. Patriot Act. And one of the excesses that is considered there is that the government may go in, without a court order, and get your library records to see what kind of books you have been reading. If we don't do something about this, someone can invade our personal computers and find out what we have been reading. So, it's the same kind of thing of invasion of personal privacy which is so important under this constitutional form of government, and under the Bill of Rights.

Now, I can tell you that my constituents are telling me, Mr. Hughes, that the spam problem is not solved. To the contrary, we better put an end to spam, and we better put an end to spyware. It's not only the problem that we don't have enough teeth in the anti-spam law, but that the perpetrator just moves offshore. So, as we address this issue of spyware we have to address the same thing. Put some teeth in the law so that they can come out with jackets over their head and be an example, but that's not going to happen if they all move offshore just like so much of the spam has, as well. So we are going to have to do something that has U.S. Government partnering with other countries to get our arms around this situation.

So let me ask you Mr. Moll, in your testimony you mentioned that spyware poses the threats to data security, which in turn, can harm our national security, elaborate on that a little bit.

Mr. MOLL. Certainly, Senator. We define spyware as inclusive of several sub-categories. Two of the more alarming include keystroke loggers and Trojans.

Key stroke loggers are simply software applications which have the ability to capture every key stroke you type at the keyboard. Products like this were recently used in an international example that, I think, highlights how effective they can be. Sumitomo Mitsui Bank's London offices were actually alleviated of $430 million in a situation where keystroke loggers were used to steal passwords, user names, and account numbers. And, this is a situation

that I think is highly relevant as it relates to national security. I already mentioned Hill Air Force Base. We have several Air Force, Navy, and Army installations that use our products to defend against this very kind of threat—installation of a key stroke logger on a system which has access to critical security information.

I would point out further that the existence of firewalls, intrusion prevention capabilities, and anti-virus capabilities today is not sufficient to defend against this kind of threat, and as a result, we effectively have offered low-hanging fruit and access to these kinds of systems through things like key stroke loggers.

The example that I offered about the Oklahoma City Sheriff's office in Kentucky, I think is a good one because the software in question that was used and found to be on those machines is a commercially available product for $99.00, you can purchase this product. If you purchase the upgrade you can actually create your own installer, which would allow you to say, create a document that you could send by e-mail, and if somebody viewed the document, it would silently install the software on that PC. That kind of capability, I think, is a great threat to our security.

Mr. SCHWARTZ. Let me say, what Mr. Moll says is illegal today under the Computer Fraud and Abuse Act. A protected computer under the Computer Fraud and Abuse Act includes a computer that holds national security information within the Government. Under any standard. The Department of Justice could be bringing these cases today. We have not seen them enforced in that way.

Senator BURNS. Mr. Schwartz, what would you like in a comprehensive approach to this, since we're talking about national security? Are we talking about electronic commerce, are we talking about consumer privacy?

Mr. SCHWARTZ. As I said in my testimony, we think that the privacy issue—I agree with what Mr. Hughes said—that the privacy issue is a separate issue. We need to deal with the general online privacy debate and get at some of these issues before they happen. We need to have that issue in a separate discussion. That said, there are things that we can do today, and enforcement of existing law is a key to it, I think, improving some of the standards that we have, seeing a better framework that pushes for improved enforcement and building incentives for positive action, are really the key points, going after behaviors instead of specific technologies is a key point here. Those are things that we can do in spyware-specific legislation, but we need to have other issues debated, we need to have oversight of some of these law enforcement agencies, and seeing what they're doing today, let's have a discussion with them about how they're using their resources and what we can do to help them use their resources and help them bring some of these cases to light, as Mr. Hughes said.

Senator BURNS. What about consumer education?

Mr. SCHWARTZ. Consumer education is an important piece of this. The problem is the debate changes very quickly. This is somewhere where anti-spyware technologies are extremely important, and we need to start doing a better job of educating consumers about security and including anti-spyware technologies in that discussion. We are working with the anti-spyware technology companies to try and build a discussion so that we can talk to consumers

in a cohesive way with some of the anti-spyware companies and with some of the consumer groups. We are just at the beginning of that discussion, but we hope to have a product by the end of the summer.

Mr. MOLL. Senator, if I may add one comment to that. I fear there is a sense that there's a silver bullet out there. We don't believe that the silver bullet is legislation. We don't believe it's enforcement, and we don't believe it's technology—particularly as it relates to things like new operating systems or new browser capabilities. Only this last week, some of what we considered to be the better browsers, and the more defensible operating systems have proven to be compromised by the likes of spyware.

What we believe is that a layered approach is important. That education, legislation, enforcement and technology need to work in concert, and I believe there's a good example now that, frankly is close to 20 years old in the antivirus marketplace. This reflects where laws have been in place, and where education to this point has been effective. You know, the market is fully penetrated by antivirus products, and that market in concert with these activities have worked well together to thwart what was once a damning problem, to make it now effectively neutralized. I think that's a good template for us to consider as we deal with this problem as well.

Senator BURNS. If the Senator would yield, I would like to add a footnote on that. When you come to awareness and public education on this problem, I would have to get a hold of some of Mr. Hughes' folks because it's going to take a pretty good word mechanic to get all the awareness and using terms that are completely strange and foreign to the majority of people, even us who use computers, into a 30 second spot, so to speak. But, nonetheless, I think some people with some cartoon ability and creativity can do that, and I know the National Ad Council would take a look at that, because it becomes, it's a very serious thing and public awareness is going to be key on this thing. We know that.

Senator Snowe, thank you for joining us this morning. We wrote you down as tardy.

[Laughter.]

Senator SNOWE. Thank you, Mr. Chairman, thank you. Well, let's just say I'm not alone in that regard.

[Laughter.]

STATEMENT OF HON. OLYMPIA J. SNOWE,
U.S. SENATOR FROM MAINE

Senator SNOWE. Thank you, Mr. Chairman, for holding this hearing today. I do appreciate it, and also for your leadership that you have given consistently over time on this issue and on the anti-spam legislation a few years ago.

I want to welcome the panelists, and Mr. Hughes, I know you're from York, Maine, beautiful. It's great to have you here. What is it? Spyware is a very insidious practice. You know, it's obviously something that's going to have to be addressed through Federal legislation in some form. Obviously we don't want to create any unintended consequences as a result of any legislative efforts and the

question is how far we go. It's gotten beyond us in terms of the magnitude of the problem.

Mr. Hughes, I know you spoke of the fact that you think we should concentrate on fraud and deception. But what is wrong with making it comparable to the "do not call" list and getting the consent of the user before this programming can be imbedded?

Mr. HUGHES. So, before you get to that analysis you need to make a decision about what you are pulling within scope. I think the NAI would strongly support transparency and accountability in download processes. The practices of drive-by downloads are simply wrong and need to be stopped. And for any download onto your computer there should be some standards of notice and choice and transparency associated with that coming onto your system.

But in defining that, in H.R. 29 in the House of Representatives, it's done under the definition of computer software. What we find is that defining it narrowly enough is a real challenge, a real challenge. I think it has been the biggest flaw that I have seen in spyware legislation to date. We cannot find a definition that is tight enough to focus only on the acute problem of spyware without creating unintended consequences.

So, I think we need to step back from the technology and have a behavioral approach. Focus on the behaviors that sit behind the technology. Those purveying spyware are simply going to move onto another technology if we eliminate their ability to use some method of software today.

Senator SNOWE. Is it because you have to make it technology-specific in the definition, or are you——

Mr. HUGHES. We have seen that in some software.

Senator SNOWE. I just know that some of the anti-spyware programs, for example, haven't even had the capability to keep up with the kind of spyware that's being developed. So, if that's problematic, how is the individual consumer going to keep up? That's the issue here. I am just afraid that this problem has gotten so great that if we don't take an aggressive approach in attacking this problem, it will get out of the hand and it will be virtually impossible.

I don't know if the legislation can ultimately define or capture all of the technology. I understand that, we authorized the Telecommunications Act in 1996, and no one could foresee to what extent it would be outdated because of the advent of so many different forms of technology, including wireless, in that process. But on the other hand, I don't see how you are going to get a hold of this problem through fraud and deception alone. I just wonder if it's going to be aggressive enough, or if there are enough resources that can be applied to the states and to the FTC to do what it needs to do to get at those who are purveying this kind of programming.

Mr. HUGHES. Senator, let me respond in two ways. First, I would concur fully with Mr. Moll in his description of a layered approach. We'd call it a holistic approach. We think that the response to spyware needs to have a number of components, legislation is clearly a component, but I think the legislative component is really more tied to the deterrent effect of enforcement, rather than the legislation itself. We also need a technology as a response. We also

need consumer education. I think the one thing missing from Mr. Moll's list is we also need industry best practices and self-regulation. In fact, those four things are the four major panels at this event that we're holding tomorrow. We are going to be examining all of those. I think we need to respond to all of those things.

The second response I would like to give you is that during the canned spam debate, the biggest area of contention was whether we go with an opt-in versus an opt-out standard. There was an enormous amount of media around that single issue. Do we require consent before you send a message or do we require you to include an opt-out in each message, so that if a consumer doesn't want to receive the next one they can say no. At the end of the day I think what we found was that substantive standard was really irrelevant to spammers, because regardless of what standard was created, they were going to go on and spam.

I think the same situation exists today with the spyware problem. We should focus on the behavior of spyware and the details around those sort of fine-tuning substantive provisions, that we should be very careful to protect legitimate uses of technology in that industry.

Senator SNOWE. Mr. Moll and Mr. Schwartz, do you think that we can conquer this problem effectively in that regard?

Mr. MOLL. Well, Senator, I think that you are correct in your belief that this is a problem that has gotten very far out of the tube, and I don't see much hope of us getting it back in. I believe that, as you state, there needs to be an aggressive approach as a result. One of the things that I included in my remarks is that we are really dealing with an organized threat, and in many ways it means that the innovation on the part of spyware today is compounded, because you have these guys working together in new ways. They create more stuff, more frequently, and it's much more innovative. I think that to try and be light-handed so, we don't ruffle the feathers of advertisers, will have an ill-effect in this regard. I think these guys are going to continue to go forward and find the edge of the law very quickly.

Mr. SCHWARTZ. Senator, I agree that transparency is an important value, and we do need to get to the point of notice and consent for software as it's delivered, and industry best practices is a good way of going about and doing that. We need to start talking about how we are going to put some of these standards in law, especially in regards to software that collects personally identifiable information. However, we do have the concern that there are some companies that are breaking existing law as it stands today, and how do we go about enforcing these new laws that we are going to put on if we can't enforce today's laws.

So, as we start to talk about what we are going to add onto this, we need to keep in mind how we're going to do enforcement down the road.

Senator SNOWE. Thank you. Thank you, Mr. Chairman.

Senator BURNS. We've got a vote coming up at 11:30, so I am going to try to ask a couple questions here, and then we will end this part of the hearing.

I was just wondering, as we look at this, Mr. Hughes, can you tell me about the various adware models that there are out there

now, in particular, what kind of user consent or notice should be given, specifically for downloads of private computers in support of adware.

Give us an idea—what's on the market out there, and Mr. Moll, you would also be a part of that, too, that's being used now and is it effective?

Mr. HUGHES. So we do not have, yet, in the adware industry, I think, a clearly defined set of best practices, but most definitely, concepts of fair information practices with notice and choice, where it is clear what is being downloaded, and how it is being downloaded, and what it's going to do once it's downloaded, and the opportunity for a consumer to consent to that practice—I think those are a absolutely necessary components for any business that is in any way interested in engaging in that.

In addition, I think an incredibly important component is the ability to get rid of it, as well. You need to have the ability to uninstall whatever you have downloaded in a way that is complete and thorough, and in a way so that it doesn't pop back up again. So, we would encourage standards like that, and I think it is one of the topics we will be discussing at length tomorrow. It's an important tool for us, I think, in defining what are appropriate standards for the adware industry.

Senator BURNS. Maybe tomorrow I should go to New York and be that little fly on the wall and take notes.

Mr. HUGHES. We would love to have you.

Senator BURNS. Mr. Moll?

Mr. MOLL. Senator, I think that today it's all over the map. We have some interesting examples that we uncovered in the last week where, once presented with the option and notification of installation of adware, you actually cannot click no. The only way to proceed without a hard reboot of your computer, is to click yes. That's a practice that we think is typical of the kinds of trickery used by adware, and by spyware more broadly.

I think it's important to look at that within the context, of three vectors of innovation we see right now coming into the industry. One of those is the means by which adware and spyware gain access to your computer. The second is the means by which they communicate—how silently they can operate, and the third is the means by which they perpetrate themselves. How deeply they can move on your system, and how hard they can be to find and remove. And I think that all three of these are elements that need to be addressed as we certainly think about best practices.

Mr. BURNS. I don't want to leave Mr. Schwartz out of this because I can see he has a comment here. There's been mention that spyware companies have posed as anti-spyware companies. Do you publish or does the industry have a list of the good actors or bad actors, is there a sort of a Better Business Bureau among your industry that people can consult?

Mr. MOLL. Senator, this is a great point. There exists one list today that's widely viewable, it's *spywarewarrior.com.* I think it's a good list, it's not well enough publicized or published. But beyond those who masquerade to be anti-spyware, while they, in fact, are spyware, a growing list of the anti-spyware companies are using the very adware networks to market themselves. And I find both

of these cases to be incredibly offensive, and a great step back for the technical solutions providers that are legitimate, like ourselves.

Senator BURNS. Mr. Schwartz?

Mr. SCHWARTZ. I agree with that last comment that it is a concern. We suggest to consumers that they read some of the more mainstream magazines about anti-spyware software. *Consumer Reports* has done some studies about anti-spyware software, CNET, Download.com, *et cetera,* have some ratings on it, so that's probably a consumer's best resource today, using a third party, reliable source to go to if you're interested in finding out more. Going back to your comment about industry, I would agree with Mr. Hughes, I'm looking forward to the discussion tomorrow as well, and we hope that it's the start of building a relationship with some of the adware companies and the networks who are all intertwined in some of this discussion.

One of the problems that we're seeing today, though, is that a lot of the companies are using illegitimate practices to gain a foothold into people's computers, so we have a base of 20 million or 50 million or 90 million computers, and then at that point they say, "We're going to change our practices now, so you shouldn't do anything about us," after they're already on these 50 million or 90 million computers. That's just not right. We do have to look at what some of these companies have done in the past and go back and see what we can do about it today.

Senator BURNS. And there's some economic value there, also, it becomes pretty expensive trying to stay ahead of the bad guys, or react to the bad guys.

Mr. MOLL. Senator that is a great point. Webroot software was only 20 people a year and a half ago, today we are fully 250 professionals, dealing solely with this problem.

Senator BURNS. That concerns me more than anything else, and then when we start adding legislation to this, it makes it even more complicated, and so we will have more questions as we move along. Congratulations on your group tomorrow, I think whenever you pull the industry together and understand the problem, and I know that you all do, and when industry takes a positive step on what we can do in the name of the consumer, because I know most of you say, "If we don't have consumers, we don't have jobs," and so we take our job of policing, and the more we know about it, it is even more serious.

I thank you for your testimony today. We will be in touch with all of you as we move this legislation. As you know, I approach these kinds of things as, do no harm, number one, and when you've got an additional farmer up here trying to deal with this, we can do harm and have some unintentional consequences that we don't want to have, to be right honest with you. So, I appreciate your testimony here today, and I appreciate your cooperation working with us, because I think it's time. I think it has implications that go way beyond just a commercial standpoint. We're dealing with something here the way people communicate and do it through my computer, in my house, that I never know anything about it. And it's bad people doing bad things to good people. And I'm very, very much concerned about that.

We're going to leave the record open for a couple of weeks, if anybody wants to make any other comments, any other Senators that want to send you questions, we would hope that you would respond to them and the Committee, and I thank you very much for your testimony here today, we stand in recess.

Hearing adjourned.

A P P E N D I X

PREPARED STATEMENT OF HON. DANIEL K. INOUYE, U.S. SENATOR FROM HAWAII

Today's hearing before the Senate Commerce Committee focuses attention on an important, and increasingly aggressive, threat to the privacy and security of the average American's computer. Specifically, today we examine the world of "spyware."

Spyware is an invasive computer software that can harvest sensitive, personal information, and can compromise the security of computer systems. In many cases, spyware is installed without the user's knowledge or consent, and even if discovered, it is removed in most instances only with great difficulty.

In some cases, spyware is merely annoying, forcing users to close unwanted pop-up ads. In other cases, however, spyware can be downloaded without a user's knowledge and used to collect personal data stored on a computer or to track an individual's web surfing habits.

The most insidious spyware programs are capable of recording a computer user's keyboard strokes to steal bank account numbers, login names, and personal passwords. This form of spyware can also make computers more vulnerable to viruses and other security breaches.

It is important that this committee consider steps that can be taken to protect consumers from spyware. For example, enforcing clear notice and consent requirements could minimize potential abuses without interfering with the creation of new and innovative technologies.

I look forward to working with my colleagues to address these difficult issues.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO C. DAVID MOLL

Question 1. You argued that the End User License Agreement is a major part of the problem in the informed consent debate. What recommendations would you suggest to improve the EULA that will help consumers make more informed decisions?

Answer. When considering a computer user's ability to make informed decisions about what programs they load onto their systems, there are many challenges posed by End User License Agreements (EULAs). There are ongoing efforts led by industry and academia to continue to refine the process of buying software online. Many companies, including Webroot, conduct usability testing to determine what language and format can be most conducive to users' willingness and ability to review the information presented to them as part of their purchase experience.

However, in spite of these efforts, there is a wide range of EULA formats and some EULAs do not clearly convey the user's authorizations and obligations with regard to the software. Some EULAs may not be readily discernable due to formatting problems that lead to confusion about the licensing terms and conditions. For example, some EULAs may be excessively long, difficult to locate, or difficult to read due to the font selected. We see companies taking advantage of this reality to gain the user's "consent," and then justify the download of the software and/or use of the user's computer resources by that software.

Ultimately, we want EULAs to be presented in clear, concise language that draws immediate attention to the terms and conditions governing the use of the software and highlights the user's authorizations and obligations with regard to the software.

Question 2. Enforcement is key in resolving the spyware issue. The anonymous nature of the Internet makes it difficult to track down the bad actors. Many argue that bad actors will not respect legislation. These skeptics believe that industry self-regulation is the preferable route to take. If Congress were to allow the industry to self regulate, how would you go about enforcing standards that the industry develops? If a bad actor is not going to abide by Federal legislation, how can industry do better?

Answer. We agree that there will be cases which are very difficult to catch in a legal net, especially those cases involving companies that are based in countries

lacking our same legal standards. The take down of what was called the "ShadowCrew," which was the topic of the May 30 *Business Week* cover story is a good example of international law enforcement and industry cooperation.

While we are seeing many instances of spyware emanating from countries outside the U.S., spyware purveyors are not solely outside the U.S.; nor are they all obvious criminals. When we assembled the list of top threats in our State of Spyware report, we found that most of the prevalent offenders are U.S. based companies. Enforcement actions like the one that the FTC brought against Seismic, help to clarify how current laws should be interpreted and applied to the spyware problem but may also be viewed as case specific.

New legislation will even further clarify the FTC's role in protecting consumers as well as the application of the FTC Act when it comes to the purveyance of spyware. Moreover, new legislation will send a strong message to people in the spyware business or funding companies that engage in bad practices that they're walking on the wrong side of the law. However, as I stated in my testimony on May 11, 2005, legislation by itself, will not remedy the problem. Any legislation that is enacted must also work in tandem with industry best practices as well as consumer education.

Question 3. A recent *Los Angeles Times* article detailed how major companies, such as Mercedes-Benz, Disney, and Dell, have inadvertently or unknowingly used adware programs in their ad campaigns. Companies purchase advertising from a provider, which then contracts out to additional providers, some of which engage in adware practices. Is there a way to address the demand side of the adware equation? How do we get companies to stop using adware as an advertising channel?

Answer. This is the area where industry efforts can make a big difference. The companies you list, and many more like them, have a tremendous amount of brand equity to protect. The Center for Democracy and Technology and the FTC are working to find ways to educate large, well-respected companies about the adware food chain and outcome of their online advertising expenditures. We are very supportive of these efforts.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO ARI SCHWARTZ

Question 1. Enforcement is key in resolving the spyware issue. The anonymous nature of the Internet makes it difficult to track down the bad actors. Many argue that bad actors will not respect legislation. These skeptics believe that industry self-regulation is the preferable route to take. If Congress were to allow the industry to self-regulate, how would you go about enforcing standards that the industry develops? If a bad actor is not going to abide by Federal legislation, how can industry do better?

Answer. Industry-developed standards can be effectively enforced in two ways:

- *Advertisers can adopt standards as prerequisites for partnering relationships*. Companies like Verizon, Dell, and Major League Baseball have developed policies for who they will advertise with. If industry-set standards serve as the basis for similar policies adopted by other large advertisers, this will create strong pressure for adware vendors to abide by those standards. Advertisers are the true customers of adware vendors. They have a unique ability to change the behavior of the adware companies.
- *Anti-spyware software vendors can use the standards as a basis for flagging or blocking programs*. As anti-spyware software increasingly becomes a standard part of computer users self-protection regimen, companies that do not abide by the standards will find it difficult to attract and retain users.

CDT believes industry initiatives thus provide a valuable supplement to strong enforcement of State and Federal laws. Private sector efforts can frustrate spyware vendors where traditional law enforcement might be difficult or where law enforcement resources are limited. They also allow for dynamic response to attempts by bad actors to create novel forms of spyware to skirt specific language in law.

Question 2. A recent *Los Angeles Times* article detailed how major companies, such as Mercedes-Benz, Disney, and Dell, have inadvertently or unknowingly used adware programs in their ad campaigns. Companies purchase advertising from a provider, which then contracts out to additional providers, some of which engage in adware practices. Is there a way to address the demand side of the adware equation? How do we get companies to stop using adware as an advertising channel?

Answer. The first step in addressing the demand side of the adware/spyware problem is to make large companies aware that their advertising dollars may be supporting adware and spyware purveyors. These companies need to be shown the negative consequences for their brands of being associated with spyware and adware practices.

Once large advertisers understand the problem, they will begin to demand that the networks and other intermediaries they partner with allow greater control over ad placement and stronger guarantees about excluding bad actors.

Spyware companies rely on business structures that make it difficult to assign culpability when malicious software is tied into ads. However, if there is demand from large advertisers, advertising brokers will work to clean up these opaque networks and provide greater transparency.

Over time, we believe improved transparency in the online advertising space and greater awareness of the adware and spyware problems will help stem the flow of money to spyware companies.