S. HRG. 109–406

REGARDING SPYWARE

HEARING

BEFORE THE

SUBCOMMITTEE ON TRADE, TOURISM, AND ECONOMIC DEVELOPMENT

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

OCTOBER 5, 2005

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

U.S. GOVERNMENT PRINTING OFFICE

27–822 PDF WASHINGTON : 2006

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

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*

SUBCOMMITTEE ON TRADE, TOURISM, AND ECONOMIC DEVELOPMENT

GORDON H. SMITH, Oregon, *Chairman*

TED STEVENS, Alaska
JOHN MCCAIN, Arizona
CONRAD BURNS, Montana
JOHN ENSIGN, Nevada
GEORGE ALLEN, Virginia
JOHN E. SUNUNU, New Hampshire
JIM DEMINT, South Carolina
DAVID VITTER, Louisiana

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

CONTENTS

REGARDING SPYWARE

WEDNESDAY, OCTOBER 5, 2005

U.S. SENATE,
SUBCOMMITTEE ON TRADE, TOURISM, AND ECONOMIC DEVELOPMENT,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:35 p.m. in room SD–562, Dirksen Senate Office Building, Hon. Gordon H. Smith, Chairman of the Subcommittee, presiding.

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

Senator SMITH. I want to thank my colleagues for being here, I know they share with me a deep interest and concern about the matter of spyware. I want to thank Chairman Majoras for rearranging her schedule to be here today.

As Chairman of the Subcommittee on Trade, Tourism, and Economic Development, which has primary jurisdiction over the Federal Trade Commission and online-privacy issues, I have a deep interest as colleagues do in spyware and have continually worked on these issues to ensure protection of consumers and businesses.

The FTC also has a responsibility to protect American consumers from all types of fraud and deception, including spyware.

According to a recent survey by the National Cyber Security Alliance, 93 percent of people feel that spyware is a serious problem, and 61 percent believe that Congress should be doing more to combat the problem. Consumers have now downloaded free versions of the two most widely used anti-spyware programs over 45 million times.

Although spyware has been used for many deceitful purposes, including theft of personal information, the technology behind it is being used also toward legitimate ends as well. I strongly believe that a total ban of an entire category of technology or product can have many unintended and serious consequences. If the definition of spyware becomes too broad, legislation adopted in haste might not take into account the evolution of future technologies, and in turn, it could stifle innovation.

I believe we must limit the abusive and deceitful practices which are allowing industry the ability to build on and improve existing technologies. To that end, I introduced the U.S. SAFE WEB Act to expand the Federal Trade Commission's current authority to enforce existing laws and allow the agency to coordinate with foreign law enforcement officials to prosecute deceptive online activities. I

have also co-sponsored legislation with Senator Allen to increase the FTC's current authority to enforce existing laws to prevent deceitful acts of spyware.

We need to give the FTC the necessary tools to go after the individuals who are already violating current Federal law. We need to address the most egregious activities and behaviors online without placing unnecessary restrictions on the entire technology industry.

Americans must be proactive in keeping our high-tech industry on the cutting edge in the world market. I believe that an appropriate balance can be found between limiting the illegitimate use of existing technologies and allowing for technology industry to grow, expand, and innovate.

As we continue to address this issue, I look forward to working with all of my colleagues to confront this growing problem appropriately and in a timely manner.

With that I'll go to Senator Nelson.

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

Senator NELSON. I'll go to praising you Senator Burns, because you and I have sponsored the bill to address spyware problems.

Senator BURNS. That's right.

Senator NELSON. Everything that Senator Smith has said is accurate. Spyware invades our privacy, leads to identity theft, exposes children to pornography, aids corporate espionage, threatens E-Commerce, and it clearly has national security implications. And technology and the private marketplace haven't found a solution to stop spyware, so we now need a tough Federal law Mr. Chairman, that clearly defines illegal conduct and gives the government more tools to go after the spyware companies.

And so Senator Burns and I are sponsoring this bill called the Spy Block Act, along with Senators Wyden, Snowe and Boxer. And last year we reported this bill out of the Committee on a unanimous vote. And it has one simple principle, empower consumers to decide for themselves what software is installed on their computers. Now Senator Allen and others have introduced another spyware bill, I think that one is a little narrow in scope but it has some very strong components. So what I want to do is, all of us to work together to merge the two approaches and get a spyware bill marked up, so we can get it moving.

The House has already passed two such bills, but it continues to wait on the Senate to act.

Thank you Mr. Chairman.

Senator SMITH. Thank you Senator Nelson, and I do look forward to working with you on this. I think we both share the belief that this is a security issue that is beyond just our individual victimization of spies and those who would invade our homes, but it also has national security implications. We simply have to work on how broad it is, so that we don't stifle the future, but that we protect people presently in our country as well.

Senator Burns.

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

Senator BURNS. Thank you very much. And thank you Mr. Chairman, for taking the leadership on this hearing today. We had a hearing before, and with most of that hearing was with the folks in the industry and consumer groups. Today I think we'll get a chance to hear from the Federal Trade Commission, which is—and will continue to have, an important role in anti-spyware enforcement actions. So the two hearings are complementary in that respect, and will help us learn more about the problem of spyware.

Also just a note, our technologies continue to grow, and the use of those technologies goes into many fields, especially in the area of electronic information and communications, with Voice over IP prominent now in the marketplace, national emergency numbers of 911 and how we apply those and protect those and the safety of 911 in emergency conditions are challenges that continue to grow for safety and security. And we must never lose sight of that. So we will continue to have problems in those areas.

Spyware, as you know, is an increasingly dangerous threat to our everyday activities in cyberspace. 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 gets downloaded into the private computers of businesses and citizens without their consent.

We also have to be careful not to throw out the baby with the bathwater, 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 online advertisements are served up to users, and what kind of consent is most appropriate. Most adware models are good for cyberspace, because it is important to have a robust and responsive advertising component for online businesses, 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 that are just trying to make cyberspace more efficient.

So I thank the Chairman of the FTC for coming up today, and I look forward to how she responds to questions, and the information she can share with us, and again to Senator Smith for setting up today's hearing, because I think it's very appropriate, and it is something that we have to get these bills moving and we need something passed and on the President's desk before Christmastime.

Senator SMITH. Thank you Senator Burns.

Senator Allen.

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

Senator ALLEN. Thank you Mr. Chairman, I especially want to thank you for calling today's hearing, and I thank Chairman Majoras for being with us today.

And I enjoyed listening to my colleagues, and maybe there will be a way that we can work together on this issue. Because the

spyware issue is one of great importance. Just to set the parameters here of what kind of a problem we have—according to the Pew Internet and American Life Project study in July of this year, in 2005 approximately 59 million American adults, nearly half of the Internet users, 43 percent say they have had spyware on their home computer.

It's irritating. It is a dangerous approach which is negatively impacting consumers confidence and harming the Internet as a viable mode, or medium for communications and also electronic commerce. And none of us here want to allow this to continue.

All of us can agree that under no circumstance is it acceptable to deceptively monitor a consumer's activities online. Unfortunately we do not all agree on how best to deal with this problem legislatively. Now in examining this offensive spyware issue, which causes so much aggravation and degrades computer performance, we need to encourage to the greatest extent possible, market driven technologies solutions, as well as strengthen the enforcement of existing laws. In my view, every legitimate business associated with the Internet has a very important interest in eliminating spyware.

A recent Federal Trade Commission report suggested that the rapid technology advancements, and this is consistent with your comments, Mr. Chairman, that there are a lot of advances in technologies to combat spyware such as firewalls, filters, anti-spyware tools and improved Internet browsers and operating systems are all the time providing easy and more affordable protections to consumers, whether at their homes or at their place of business.

I think that the Internet's viability is being challenged by this deceptive spyware though, and because of these fraudulent and deceptive installations of spyware programs being a concern, it is not a concern though whether this is legal or not; this already is illegal under Federal law, it's a violation of Federal law. Such as the Federal Trade Commission Act, and the Computer Fraud and Abuse Act.

So I think Congress needs to focus its efforts on adequate resources and penalties to combat this criminal activity. I've determined that Federal officials, and we'll hear from the Chairman, believe that 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 a lack of overall resources. That's why my legislation, S. 1004 with the support of you Mr. Chairman, Senators Smith, Sununu, Ensign, and Enzi, provides Federal law enforcement officials with the resources and the tool necessary to increase the breadth and the strength of anti-spyware enforcement efforts.

Our legislation strikes a careful balance that you talked about Mr. Chairman, between 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, our legislation sets a national standard. It doesn't matter what state you're in, or territory of the United States. There ought to be that national standard for the unfair and deceptive practices associated with spyware. Additionally, our legislation provides the FTC with the

authority to share and coordinate information with foreign law enforcement officials to improve their ability to bring cases and prosecute international spyware purveyors, your separate bill, Mr. Chairman, this is just a component of our bill, but yours covers it as well.

But lastly, our legislation addresses the most egregious activities and wrongful behavior conducted via spyware, by significantly increasing civil and criminal penalties including disgorgement. We need to ensure that law enforcement officials can get after the illegal gains of these criminals. You can fine them, but if they have any assets that are traceable to this illegal activity it is an enterprise on their part, and they're selling this information. And we ought to get after those ill gotten gains. I don't care what it is, bank accounts, yachts, art objects, whatever they've bought, we need to get after these enterprises as well as the criminal and civil fines.

I believe again, that we need to find some market driven solutions, technology solutions that will ultimately solve this problem. I want to help the FTC have the resources they need to get after this criminal and illegal behavior, and I look forward Mr. Chairman to hearing from the Chairman of the FTC, but most importantly if there is a way, and I'm not sure there is, there are some just fundamental differences, but we need to act.

The Senate a lot of the times is the last to act, but I think there's enough will here that I hope working with my good friend Senator Burns that we can hopefully find a common ground to have the Federal Government help the FTC do its job, set a national standard and get you the resources to get after this illegal behavior.

And I thank you again Mr. Chairman.

Senator SMITH. Thank you very much Senator Allen. Madam Chairman, the mike is yours, we look forward to your testimony.

STATEMENT OF HON. DEBORAH P. MAJORAS, CHAIRMAN, FEDERAL TRADE COMMISSION

Ms. MAJORAS. Thank you very much Mr. Chairman, and Members of the Subcommittee, and good afternoon.

The Federal Trade Commission appreciates this opportunity to provide the Commission's views on the serious problems that spyware is causing to consumers and the steps that the FTC has taken to address the problem.

Although the views expressed in the written testimony present the views expressed of the Commission, my oral presentation and responses to questions are my own, and may not necessarily represent the views of the Commission.

As the Subcommittee is aware, the Commission has a broad mandate to prohibit unfair competition, and unfair or deceptive practices in the marketplace. We have actively used this authority to address consumer problems on the Internet, including Internet fraud, privacy, spam and spyware.

The term spyware can be difficult to define. It is ordinarily thought of as including programs such as keyloggers, that can copy information from consumers' computers, as well as some types of adware, software that monitors computers' surfing habits and then serves up pop-up advertisements.

At the FTC, our focus is on spyware and other malware that is downloaded without authorization, and causes consumers harm. The consumer harm from spyware can range from the capture of sensitive personal information to degradation of computer performance, to the nuisance and distraction of popup ads.

To address spyware, we implemented an active program, combining law enforcement and consumer education supplemented by our research. Much of the harmful conduct associated with spyware is already illegal. Indeed the FTC has brought several cases, and today is announcing it has filed another action, *FTC* versus *Odysseus Marketing*. In this case, we filed a complaint in Federal District Court in New Hampshire against Odysseus Marketing and its principal, Walter Rines, charging them with secretly installing spyware on consumers' computers.

Our complaint alleges that the defendants deceptively market and distribute a bogus program called Kazanon, which defendants claim will make users anonymous when using peer-to-peer file-sharing programs.

Not only does Kazanon not work as promised, which itself a violation of the FTC Act, but it also automatically installs a spyware program called Clientman on the users' computer. Clientman in turn automatically installs numerous adware and other programs on behalf of others. And this spyware, among other things, replaces or reformats Internet search engine results, generates pop-up ads, and captures and transmits information which may include personal information.

Our complaint alleges that defendants have failed to disclose adequately that downloading Kazanon will install this spyware. In fact, the only place that Clientman's virtual takeover of the host computer is disclosed is in the end user license agreement, or as we call it the EULA.

Consumers, however, do not need to view the EULA in order to download Kazanon, and even if they did they would have to wade through five paragraphs of dense text before they reached information even approaching the disclosure.

We further allege that once Clientman is installed, consumers cannot remove Kazanon and Clientman from their computers through reasonable means. Programs do not appear on the desktop or in the start menu, and because they avoid being detected by the Microsoft Windows operating system, consumers cannot use Microsoft's default uninstall utilities to remove them.

And defendants claim to provide an uninstall tool, but it doesn't work. In fact, we allege in the complaint that if you activate defendants' uninstall tool, typically that will result in having additional files being added to your computer.

Now as we bring each spyware case, we learn more about the technology and tricks in the industry and we increase our ability to bring future cases. We've made spyware investigations and prosecutions an enforcement priority and we will file more law enforcement actions. There's no question however that attacking spyware is challenging.

Given its surreptitious nature, it is often difficult to ascertain from whom, from where, and how spyware is disseminated. Many

who distribute spyware are adept at hiding, covering their tracks, and evading responsibility.

Further, consumer complaints about spyware are less likely to lead us directly to law enforcement targets than some other complaints. Consumers often do not know from where the spyware has come, or even that it was spyware that caused the problems to their computers in the first place.

There are five additional points that the Commission believes are important to our continuing efforts to combat the dissemination of spyware.

First, many spyware distributors and other Internet scam artists are located abroad, or mask their location by using foreign intermediaries to peddle their scams. A majority of spyware programs distributed to the United States consumers come from foreign distributors. In the FTC's investigations, staff finds that regardless of where the spyware distributors are physically located they are often using foreign Internet service providers, or web hosting companies, or domain registrars, which makes it difficult to crack down on who's ultimately responsible.

Our ability to pursue distributors of spyware, and spam and other Internet threats would be significantly improved if Congress were pass the U.S. SAFE WEB Act. And Chairman Smith, we thank you for introducing S. 1608 which would give us that needed authority.

Second, coordinated effort at the Federal and State level is essential. The Commission is continuing to cooperate with Federal and state partners, which now are bringing law enforcement actions against spyware distributors. At the Federal level, the Department of Justice is able to prosecute criminally those who distribute spyware in certain circumstances. And at the State level, state attorneys general are bringing civil law enforcement actions and both are critical complements to the FTC's actions.

Third, an educated consumer is perhaps the best defense against online fraud and spyware. Over the last few months the FTC has taken a broader look at its educational materials and tactics related to cyber security, online privacy, and Internet fraud, and we've updated our messages and outreach strategies to better educate consumers about these important issues.

Just last week the Commission launched a new consumer ed initiative, OnGuard Online. It has general information on online safety, as well as sections with specific information on a range of topics, including spyware, and with the Chairman's indulgence in a few moments we'll give you a quick demonstration of this new website.

Fourth, the Commission believes that legislation granting the Commission authority to seek civil penalties against spyware distributors would be useful in deterring the dissemination of spyware. The Commission has the authority, as Senator Allen referred, to file actions against those engaged in conduct in Federal Court, and we have the authority to obtain injunctive relief, including monetary relief in the form of consumer redress, or disgorgement of ill gotten profits.

But in some instances it may be difficult for us to prove the sort of financial harm that we would need to in order to get that sort

of redress. A civil penalty is often then the most appropriate remedy in those cases, and we believe it could serve as a strong deterrent as well.

And finally, as with any technology problem, the most comprehensive response may have to come from new technology. Technology is what got us here, and technology should be able to bring us out eventually. As in other areas like spam and data security, it is essential that industry continue to develop technology to assist their own customers in combating the threats of spyware and other malware.

We know that ISPs and other industry members are developing responses to consumer concerns about spyware and we also are appreciative that they have provided the Commission with important assistance in our investigations.

In conclusion, Mr. Chairman, I assure you that the FTC will continue to aggressively attack spyware with law enforcement actions and with innovative consumer education. And we look forward to working with the Committee on the problem of spyware.

Now I look forward to answering any questions you have, but before we begin, if it's still all right with you, Mr. Chairman, I'd like to ask Nat Wood, who's our Assistant Director for Consumer and Business Education, to just give you a brief demonstration of our new OnGuardOnline.gov website, particularly as it relates to spyware.

All right. What you're seeing before you is the result of team work. The FTC, a number of other Federal agencies, and the technology community have teamed up to create OnGuardOnline.gov, which is a new site to help computer users guard against Internet fraud, secure their computers and protect their personal information. We're encouraging companies and other organizations to help fight spyware, spam, identity theft and the like, by sharing the tips on this website with their employees, their customers, members and constituents.

Interestingly, this website is branded independently of the FTC. We are not making it FTC materials, because we want any organization with an interest, whether it's government, business, consumer groups, whatever, to take this, make it their own and distribute it widely across our country. Indeed, we now have a lot of interest that's coming from other organizations around the world who would like to be able to use these materials.

So just quickly looking at the home page, probably the most important part of this is the seven practices for safer computing. These are practices that we want consumers to be using regardless of what they're doing online. These are general tips. The site also contains a link on which consumers can click if they want to receive free e-mail alerts from the Department of Homeland Security on various threats to the online world.

Then we have the "Learn About" section, in which consumers can click on various modules to learn about different threats and the like, so there you see we clicked on identity theft, there's one on phishing, we've done this in a flexible way, so that as new threats develop we can add them to the website. And then we have an "About Us" page, which if you click on that gives you, gives the consumer, a description of all of the various Federal agencies and

other organizations that they can turn to for help with respect to their online problems. So going back to the modules, we'll just turn quickly to the spyware section, and what you can see if you click on this section, is first and foremost you get a quick tips section, which tells consumers very quickly what they should do, then below that we have a much longer article, so that if consumers want to read further about spyware, its dangers and what they can do about it, they have that there.

We have a place for links and resources so that they can link to additional anti-spyware resources, including if they want to learn about what anti-spyware tools are available. And then we have a section that tells the consumer where to report spyware problems and, not surprisingly, the FTC is listed there. Then because we know and experts have told us, and we did a lot of consumer testing, and the like, we know the folks who spend a lot of time online like to be interactive online, so if they think they're experts we have a quiz.

So you click on this to begin the quiz. You get a little bit of information about spyware and then the quiz goes on to ask various questions to educate the consumers. So this one says a pop-up ad appears on your computer screen offering an anti-spyware product, "what's your best course of action?" And then gives various answers, I would click on "C" which says "close the window if you want spyware protection software, get it from a provider you know and trust." And that would be—I would then hear, "Excellent choice. The scammers will have to get up pretty early in the morning to pull one over on you," and the quiz goes on. And obviously if you get the answer wrong we explain why, in fact that would be wrong, and give the better course.

So this is—we will have quizzes on all of the modules very soon, and I'm also pleased to report that this is also available in Spanish.

So thank you very much Mr. Chairman.

[The prepared statement of Ms. Majoras follows:]

PREPARED STATEMENT OF HON. DEBORAH P. MAJORAS, CHAIRMAN, FEDERAL TRADE COMMISSION

I. Introduction

Mr. Chairman and Members of the Committee, the Federal Trade Commission ("Commission" or "FTC") appreciates this opportunity to provide the Commission's views on "spyware."[1] Spyware is a serious and growing problem that is causing substantial harm to consumers and to the Internet as a medium of communication and commerce. Preventing spyware that causes such harms is a priority for the Commission. We welcome this chance to describe what the FTC is doing to try to protect consumers from these harms.

The Commission has a broad mandate to prevent unfair competition and unfair or deceptive acts or practices in the marketplace. Section 5 of the Federal Trade Commission Act gives the agency the authority to challenge acts and practices in or affecting commerce that are unfair or deceptive.[2] The FTC's law enforcement activities against unfair or deceptive acts and practices are generally designed to promote informed consumer choice, because an informed consumer is an empowered consumer.

Spyware and other "malware" that is downloaded without authorization can cause a range of problems for computer users, from nuisance adware that delivers pop-

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

[2] 15 U.S.C. § 45.

up ads, to software that causes sluggish computer performance, to keystroke loggers that capture sensitive information. As described below, the Commission has an active program to address concerns about spyware and other malware, including research, law enforcement and consumer education. In the past year, the Commission has initiated five law enforcement actions addressing spyware and malware, and has ongoing investigations. Moreover, as in other areas such as spam and data security, we believe that it is essential that industry continue to develop technology to assist its customers in combatting spyware.

II. Spyware Law Enforcement

One of the FTC's first steps in responding to the spyware problem was to educate ourselves in order to develop, implement, and advocate effective policies to respond to it. In 2004, the FTC sponsored a public workshop entitled "Monitoring Software on Your PC: Spyware, Adware, and Other Software." The agency received almost 800 comments in connection with the workshop, and 34 representatives from the computer and software industries, trade associations, consumer advocacy groups and various governmental entities participated as panelists. In March 2005, the FTC released a staff report based on the information received in connection with the workshop.[3] Notwithstanding significant challenges in defining "spyware,"[4] the staff report recommended that the government should: (1) increase, using existing laws, criminal and civil prosecution of those who distribute spyware; and (2) increase efforts to educate consumers about the risks of spyware. The Commission is pleased to be able to describe today what we are doing to implement these recommendations.

The Commission's spyware law enforcement strategy focuses on three key questions. First, were consumers aware of the installation of the software on their computers? Second, what harm did the installation of the software cause? Third, how difficult was it for consumers to uninstall the software after it had been installed?

A. Did Consumers Know?

A common problem with spyware is that it is installed on consumers' computers without their knowledge. Some spyware distributors use so-called "drive-by" downloads to install their software on computers without even any pretense of obtaining consent. In *FTC* v. *Seismic Entertainment,*[5] for example, the Commission alleged that the defendants exploited a known vulnerability in the Internet Explorer web browser to download spyware to users' computers without their knowledge. The FTC alleged that this was an unfair act or practice in violation of Section 5 of the FTC Act, and a Federal district court entered a preliminary injunction that prohibited the defendants from using this method to distribute their software.

In other instances, software distributors may violate Section 5 of the FTC Act by failing to disclose clearly and conspicuously to consumers the software that is being installed. In *FTC* v. *Odysseus Marketing, Inc.,*[6] the defendants offered consumers a free software program that purported to make the consumers anonymous when using peer-to-peer file sharing programs. The Commission alleged, however, the distributors failed to disclose to consumers that this program, in turn, would install other, harmful software on their computers. The Commission recently filed a complaint in Federal court alleging that this failure to disclose was deceptive in violation of Section 5 of the FTC Act, and we are awaiting a ruling on our motion for a temporary restraining order. Similarly, in the *Advertising.com, Inc.* case,[7] the respondents allegedly offered free security software, but failed to clearly and conspicu-

---

[3] The workshop agenda, transcript, panelist presentations, and public comments received by the Commission are available at *http://www.ftc.gov/bcp/workshops/spyware/index.htm.* The FTC Staff Report, Monitoring Software on Your PC: Spyware, Adware, and Other Software, released Mar. 2005, is available at *http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf.*

[4] At the FTC workshop, there was "broad agreement that spyware should be defined to include software installed without adequate consent from the user," yet there remained "substantial differences of opinion as to what distributors must do to obtain such consent." *See* FTC Staff Report, *supra* note 3, at 4–5. In addition, there was agreement that "to avoid inadvertently including software that is benign or beneficial, the term spyware should be limited to software that causes some harm to consumers," although there were "substantial differences of opinion as to when software has caused the type and magnitude of harm to warrant being treated as spyware." *Id.* The FTC staff therefore concluded that "these fundamental issues of consent and harm need to be resolved before any common definition of spyware can be developed." *Id.* at 5.

[5] *FTC* v. *Seismic Entertainment, Inc.,* No. 04–377–JD, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004).

[6] *FTC* v. *Odysseus Marketing, Inc.,* No. 05–CV–330 (D.N.H. filed Sept. 21, 2005).

[7] *In the Matter of Advertising.com,* FTC File No. 042 3196 (filed Sept. 12, 2005), available at *http://www.ftc.gov/os/caselist/0423196/0423196.htm.*

ously disclose to consumers that bundled with it was software that traced consumers' Internet browsing and force-fed them pop-up advertising. The Commission recently issued a final consent order to resolve administrative complaint allegations that this failure to disclose was deceptive in violation of Section 5 of the FTC Act.

The Commission's spyware law enforcement actions reaffirm the principle that consumers have the right to decide whether to install new software on their computers. Acts and practices that undermine their ability to make this choice will be vigorously prosecuted.

B. Substantial Harm to Consumers

As the Agency learned at the workshop, and through our enforcement actions and subsequent investigations, spyware can cause a broad range of injury to consumers. The harm from spyware may vary significantly in both type and severity.

The allegations in the *Seismic* case describe a prime example of software causing several types of serious harm to consumers. The software allegedly changed the consumer's browser home page and default search engine, displayed an incessant stream of pop-up ads, and caused the user's computer to malfunction, slow down, or crash. But perhaps the most serious harm alleged was that the spyware secretly installed a number of additional software programs, including programs that could monitor Internet activity and capture personal information entered into online forms.

Another example of serious harm to consumers allegedly caused by spyware arose in the *Odysseus* case. According to the Commission's complaint, the defendants surreptitiously install a spyware program called "Clientman " on the computers of consumers. Clientman, in turn, installs a number of adware and other programs. It also replaces or reformats Internet search engine results, generates pop-up ads, and captures and transmits information, which may include personal information.

In the *Advertising.com* case, the Commission alleged that software bundled with free security software collected information about consumers, including the websites they visited, and then was used to send a substantial number of pop-up ads. Although the harm to an individual consumer from receiving such pop-ups ads may be less egregious than the harm in other FTC spyware cases to date, the harm to consumers in the aggregate from these pop-up ads was sufficient to warrant law enforcement action. The Commission alleged a violation of Section 5 of the FTC Act because the presence of bundled adware that collected information about consumers' computer use and led to numerous pop-up ads clearly would have been material to consumers in determining whether to install the free security software.

As stated in the FTC staff spyware report, it is the combination of lack of knowledge and consumer harm that makes certain installation of software illegal under the FTC Act. [8]

C. Uninstalling and Deleting Spyware Problems

As described above, spyware often is installed without consumers' knowledge and causes consumers substantial harm. This type of installation should not occur, but once it has, consumers should be able to uninstall or disable such software. Unfortunately, the FTC's law enforcement experience and research shows that some software distributors take improper advantage of consumers' concerns about spyware and market bogus anti-spyware tools. In addition, in the FTC's experience, some spyware programs are difficult to identify and uninstall or disable.

Many consumers who want to determine whether there is spyware on their personal computers acquire and run an anti-spyware program. An anti-spyware program usually identifies each software program that it concludes is spyware and then gives the consumer the option of deleting it. Some software distributors, however, take advantage of consumers looking for anti-spyware products by falsely representing to consumers that spyware resides on their computers and making false claims about the ability of their products to remove spyware. In two recent cases, *FTC* v. *MaxTheater* and *FTC* v. *Trustsoft,* [9] the FTC alleged that the defendants made false claims to consumers about the existence of spyware on their machines. According to the FTC's complaint, the defendants then used these false claims to convince consumers to conduct free "scans" of their computers. These scans identified innocuous software as spyware, helping to persuade consumers to purchase defendants' spyware removal products at a cost of between $30 and $40. Moreover, the FTC alleged, the defendants claimed their spyware removal products could effec-

---

[8] *See generally,* FTC Staff Report, *supra* note 3, at 20–21.

[9] *FTC* v. *MaxTheater, Inc.,* No. 05–CV–0069 (E.D. Wa. filed Mar. 7, 2005), available at *http://www.ftc.gov/opa/2005/03/maxtheater.htm*; *FTC* v. *Trustsoft, Inc.,* No. H–05–1905 (S.D.Tex. filed May 31, 2005), available at *http://www.ftc.gov/opa/2005/06/trustsoft.htm.*

tively uninstall many different types of known spyware programs, but the defendants' products did not perform as promised. The Commission filed actions alleging that the perpetrators of these scams violated Section 5 of the FTC Act, and the courts have entered preliminary injunctions in both cases that prohibit the claims.

Software falsely billed as an anti-spyware product certainly can make it difficult for consumers to identify and uninstall or disable spyware programs. Furthermore, even if consumers can identify spyware programs, some of them are particularly difficult to remove or disable. In the *Odysseus* case, the complaint alleged that consumers could not uninstall the software through any reasonable means, such as by using the standard "Add/Remove" program on the Microsoft Windows operating system. According to the Commission's complaint, although the defendants purport to provide instructions for uninstalling the program, those instructions are not only extremely difficult for consumers to find, they simply do not work. The complaint alleged that the defendants' failure to provide users with a reasonable means to locate and remove the program is an unfair act or practice in violation of Section 5 of the FTC Act.

The FTC's law enforcement actions under Section 5 of the FTC Act have focused on preserving consumers' ability to decide what software programs to install and retain on their computers, and preventing substantial harm from software programs installed or remaining against the consumers' wishes.

III. Additional Steps to Address Spyware

Given the prevalence of spyware and the consumer harm it inflicts, the FTC has made spyware investigations and prosecutions an enforcement priority, and we will continue to file law enforcement actions against those who distribute spyware in violation of the FTC Act. The Commission would like to emphasize four additional measures that it believes would enhance its efforts to combat the dissemination of spyware.

First, the FTC supports legislation that would enhance its ability to investigate and prosecute spyware distributors that are located abroad or who try to mask their location by using foreign intermediaries to peddle their scams. Webroot, a well-known anti-spyware product distributor, recently reported that a majority of spyware programs distributed to United States consumers come from foreign distributors.[10] In the FTC's investigations, staff finds that, regardless of where spyware distributors are physically located, they often use foreign Internet service providers, web hosting companies, and domain registrars to create their websites, so that it is difficult for the agency to track down who is ultimately responsible.

The FTC's ability to pursue distributors of spyware, spam, and other Internet threats to consumers would be significantly improved if the Congress were to pass the U.S. SAFE WEB Act, introduced by Chairman Smith in the Senate as S. 1608. The Act makes it easier for the FTC to share information and otherwise cooperate with foreign law enforcement officials. The Internet knows no boundaries, and it is critical to improve the FTC's ability to work with the officials of other countries to prevent online conduct that undermines consumer confidence in the Internet as a medium of communication and commerce.

Second, the Commission will continue to coordinate with its Federal and state partners who are starting to bring their own law enforcement actions against spyware distributors to make law enforcement as effective as possible. At the Federal level, the Department of Justice is able to prosecute criminally those who distribute spyware in certain circumstances. In August 2005, for instance, the Department announced the indictments of the creator and marketer of a spyware program called "Loverspy " and four others who used the program to break into computers and illegally intercept the electronic communications of others.[11] At the state level, state attorneys general are bringing civil law enforcement actions. Federal criminal and state law enforcement actions are a critical complement to the FTC's law enforcement actions.

Third, the FTC and others need to continue to play an active role in educating consumers about the risks of spyware and anti-spyware tools. The FTC has issued a Consumer Alert specifically on spyware, as well as four other Alerts addressing other online security issues such as viruses and peer-to-peer file sharing. The Spyware Alert lists clues that indicate spyware may have been installed and also discusses measures consumers can take to get rid of spyware or to reduce their

---

[10] Webroot Software, Inc., State of Spyware Q2 2005, released Aug. 2005, at 26, available at *http://www.webroot.com/land/sosreport.php.*

[11] Press Release, Department of Justice, Office of the United States Attorney, Southern District of California Carol C. Lam, News Release Summary (Aug. 26, 2005), available at *http://www.usdoj.gov/usao/cas/pr/cas50826.1.pdf.*

chances of getting spyware in the first place. The Spyware Alert has been accessed over 100,000 times since it was released in October 2004, and the tips it includes have been repeated in dozens of print and broadcast media stories.

And, just last week, the Commission launched a new consumer education initiative, OnGuard Online. Over the past few months, the FTC staff has taken a broader look at its education materials and tactics related to cybersecurity, online privacy, and Internet fraud, and updated its messages and outreach strategies to better educate computer users about these important issues. The FTC's new website—OnGuardOnline.gov—has general information on online safety, as well as sections with specific information on a range of topics, including spyware. This structure allows us to add to the site as new topics arise. The spyware module includes up-to-date information, as well as interactive features like quizzes and videos. The FTC has also printed a million copies of a brochure, "Stop Think Click: 7 Practices for Safer Computing," with information on spyware and other computer safety topics. The site and the brochure have information on various technologies, but the agency is also emphasizing behavioral changes that computer users can make to stay safe online—for example "protect your personal information," and "know who you're dealing with." By taking this approach, the FTC can ensure that the tips remain relevant even as technology evolves.

Our partners in the OnGuard Online initiative include: the Department of Homeland Security, the U.S. Postal Inspection Service, the Department of Commerce, Technology Administration, the Internet Education Foundation, the National Cyber Security Alliance, the Anti-Phishing Working Group, TRUSTe, iSafe, AARP, the National Consumers League, and the Better Business Bureaus. In an effort to ensure maximum distribution of these materials, we have not branded them as our own. Instead, we are encouraging any organization interested in computer security to link to OnGuardOnline.gov, distribute our free brochure, or reprint the OnGuard Online materials.

Fourth and finally, the Commission believes that legislation granting the Commission authority to seek civil penalties against spyware distributors may be useful in deterring the dissemination of spyware. As described above, the Commission has challenged conduct related to spyware dissemination as unfair or deceptive acts or practices in violation of Section 5 of the FTC Act. Under Section 13(b) of the FTC Act, the Commission has the authority to file actions against those engaged in this conduct in Federal district court and obtain injunctive relief, including monetary relief in the form of consumer redress or disgorgement of ill-gotten profits. However, it may be difficult in some instances for the FTC to prove the sort of financial harm to consumers needed to order consumer redress, or the ill-gotten gains necessary to order disgorgement. A civil penalty is often the most appropriate remedy in such cases, and serves as a strong deterrent.

IV. Technological Solutions

Reducing the problems associated with spyware and other malware will require the efforts of government, consumers, and industry acting both individually and in concert. As in other high-technology areas, the best and most comprehensive responses to misuse of technology will often be improved technology. At this time there are certain technologies consumers can use to help protect themselves, but none is completely effective and further developments are needed to enhance security.

The primary technological tools that consumers can use right now to protect themselves from spyware are detection programs. These programs can scan consumers' computers, inform them whether there is spyware, and offer them the option of disabling it, deleting it, or leaving it alone. To be effective, however, these programs must be updated on a regular basis. In addition, they are inherently variable depending on what they classify as "spyware." Furthermore, they only detect spyware once it has been installed; they do not prevent its installation. Some Internet service providers have made spyware scanners and removers available to their subscribers. Firewalls also provide some protection from spyware, but, like scanners, they do not prevent spyware from being installed. Rather, they alert consumers if installed spyware attempts to send out information it has collected.

Other technological solutions at the browser and operating system level are being developed. The Commission's experience in other technological areas suggests that market forces will provide the high-tech industry with incentives to develop technological solutions, although it is not clear exactly what that technology will be or when it will be available.

V. Conclusion

The FTC will continue to execute aggressive law enforcement and innovative consumer education programs in the spyware arena. The FTC thanks this Committee for focusing attention on this important issue, and for giving me an opportunity to discuss the Commission's enforcement program. The Commission looks forward to working with the Committee on the problem of spyware.

Senator SMITH. Thank you Ms. Majoras. I assume from your testimony that the FTC could use some more authority, because it supports the Allen bill that I've introduced with him. Is that accurate, you could use some more authority to do more rulemaking on this issue?

Ms. MAJORAS. Well, we could, as you and Senator Allen have pointed out, we do believe that we have legal authority to attack spyware and we've already done it in five different cases, but we would like additional authority to work with our counterparts overseas, we think that's absolutely critical and we think we really could use civil penalty authority to assist us in bringing actions and remedying them.

Senator SMITH. And how about more resources? If you had your druthers would you be getting more authority or more resources to prosecute cases?

Ms. MAJORAS. That's always a tough question whether we need more resources. We work very hard on the budget process with Congress to get whatever resources we think we're going to need for the year. It's tough for me to turn down more resources if they're being offered. But I don't think—resources have been less a problem than I think, folks are concerned about the bigger problem, which has been finding the folks who are distributing the spyware and then being able to serve them. They obviously can hide behind the Internet, they can skip town, they can skip the country, they go to other countries and hide, and that has actually been the biggest problem. We are using our resources as wisely as we can. We are squeezing every bit we can out of every dollar, and our anti-spyware program is part of the larger program that includes spam, and Internet fraud, on which we're devoting substantial resources.

Senator SMITH. What percentage would be coming into our country from abroad, and what percentage starts here in the United States?

Ms. MAJORAS. We don't have exact percentages, it's very hard to tell. But certainly we think a great majority of spyware is either coming in from outside the United States, or is making use of a foreign intermediary in some way to attack consumers in the United States.

Senator SMITH. And in the global economy in which we live, you need more authority to deal with the international component, I think that has been very clearly demonstrated.

Senator Nelson.

Senator BILL NELSON. Good afternoon Madam Chairman. Tell me if you agree with the following statement of principles, that software should not be installed without a consumers knowledge and consent.

Ms. MAJORAS. If it harms consumers, I do agree with that.

Senator BILL NELSON. Consumers should know who is installing the software on their computer.

Ms. MAJORAS. Generally, yes.

Senator BILL NELSON. Consumers should have the ability to completely remove software from their computers.

Ms. MAJORAS. Again, most of it, yes.

Senator BILL NELSON. If software is going to collect information about a consumer, the software should inform the consumer first.

Ms. MAJORAS. Generally yes.

Senator BILL NELSON. If software is going to cause ads to appear it should make clear what is causing the ads.

Ms. MAJORAS. That one is a little bit trickier, we have taken that on a case-by-case basis.

Senator BILL NELSON. In your testimony, we're going to—you've addressed it and we've got to confront the question of preemption. Do you think that it's important to preserve general state consumer protection laws as potential state-level tools against software?

Ms. MAJORAS. We do. In almost any context, we support allowing the state attorneys general to continue to enforce their consumer protection statutes. Having said that, there are certainly instances in which businesses really need consistent—if businesses are going to get guidance, we all benefit if it's consistent across the Nation.

Senator BILL NELSON. Do you think it would be helpful to have some baseline standards for what kind of behavior is acceptable, what disclosures should be given to consumers, and a statement of the right to uninstall software?

Ms. MAJORAS. Well, with respect to disclosures, the FTC has provided general guidance to companies for a number of years in the form of something we call Dot Com Disclosures, so we've already provided some general guidance. Our only concern about making the guidance too specific Senator Nelson, is that the landscape keeps changing and those who insist on perpetrating fraud and harming consumers find new ways to do it. And so the concern with being too specific about what is permitted and what isn't, not only is you have to get the words exactly right, so that you don't prevent what should be legal conduct, but also we have to worry about the future, and we don't want to bring a case, and only to be told, well, because that particular practice wasn't specifically listed in the piece of legislation, therefore the FTC cannot attack it.

Senator BILL NELSON. I understand. I'm talking about more baseline standards, on behaviors, on disclosures, and on the right to uninstall.

Ms. MAJORAS. We think the FTC has put a lot of that out there, but yes, there's no question that business can always use guidance, and those businesses who actually have an interest in complying with the law.

Senator BILL NELSON. And give us your opinion about the basic right of a consumer to have the ability to remove software from his or her computer?

Ms. MAJORAS. Well, we've actually brought cases in which we have alleged violations of the FTC Act because consumers do not have that right, including the case that I mentioned earlier today, Odysseus Marketing. So we do think it is a violation if software is

downloaded to a consumer's computer that is causing some harm, and the consumer cannot find a reasonable means to remove it.

Senator BILL NELSON. Thank you.

Senator SMITH. Senator Burns.

Senator BURNS. Madam Chairman, thank you again for coming today. You're probably aware that there are several industry groups working on definitions of spyware. It always seems like when we get into these kind of situations we all define the same thing in different ways and usually definitions are what lawyers make a living at, and enforcement becomes more difficult. To what degree, do you think the FTC can work with these industry groups, and to get efforts underway and do you think it is important that we have a public rulemaking process? We all say awareness is everything, and a public process in which we make the rules and then we define the terms. What's your attitude toward a situation like that?

Ms. MAJORAS. Well, I certainly think that working together with industry is critical in attacking spyware and obviously if legislation is being considered it's critical because these folks are the experts. And they can tell us, not only explain to us not only what's out there today, but they're also thinking several steps ahead. And that can be very important if we're trying to put in place rules that are going to work on a going forward basis. So I think that can be very important. One thing I would caution against though is I know that many in industry have been anxious to really come up with the definition of spyware. And I think part of the reason why it's been difficult to come up with a definition that everyone can agree on is again, because we have a bit of a moving target. And so what we've tried to do at the FTC is we're really looking at two things: whether the software has been downloaded without the consumer's permission, and causes some substantial harm to the consumer; that is really what we've been operating under. Call it spyware, call it adware, call it malware, that is what we have been looking at when we bring a case.

Senator BURNS. And also on the awareness, that same thing, now you've got some proceedings going on for consumers. Can you tell us how those proceedings are going, were there fines levied where if individual consumers, their computers were hurt, or crashed, did they get compensated, their computers back up and running again, or new hard drive, or whatever. Did they get their money back on their software of whatever, can you give us some kind of an idea of the results you've had in these proceedings?

Ms. MAJORAS. Yes Senator, we've brought five cases since last October, both the first case, and the last case we brought are still in litigation. In the first case we brought we were able to get a preliminary injunction against the conduct and that was a case in which we alleged in the complaint that in fact, yes, the purveyor of the spyware hijacked the consumers' computers and changed their settings and the like, changed their home pages, and downloaded personal information. That case is still in litigation, similarly obviously we've just announced the case we filed last week, in which spyware was downloaded without consumers' permission and again, essentially in this case what we allege in the complaint is that it has taken over the consumer's computer. That's

still in litigation. We've brought a couple of cases against those who claim that they're selling an anti-spyware solution, when in fact it's a solution that doesn't work, and so in those two instances both of those respondents did settle those cases with us, and we were able to get some consumer redress, if I recall correctly.

And we brought one additional case in which the respondent advertised a free download of security software. But then didn't tell consumers that if they downloaded this free security software they would also get adware attached to their computer, so then they would be barraged with pop-up ads and the like and that case also settled.

Senator BURNS. In other words they used the spy block technology to implant their own adware stuff without telling the customers, is that correct?

Ms. MAJORAS. I'm not sure which technology they used, but without sufficient disclosure to the consumer they did download adware to the computer.

Senator BURNS. Now since these proceedings have been filed and you've been in them, are there any surprises about—do you have resources to take the case to final?

Ms. MAJORAS. We do have resources I think to take these cases to final. The biggest surprises probably have been—really probably came in the beginning. We started trying to figure out a way how we were going to investigate these cases and we infected two of our own computers so badly with spyware that they couldn't be used anymore and so we learned a lot. And so one of the things we've done during this time period as we've been bringing these cases is, we've bought some new computers, some new software, and some new hardware to assist us in going forward. As I said, we're learning as we go through this.

Senator BURNS. Well, I thank you for your work. And I don't think there's a person up here today that doesn't want to get you some legislation and empower with you a little more power than you have now, because I think you're on the right track. And also the differences that we have, we'll get those worked out and I would hope that we could have something on the President's desk and for you to look at pretty quickly. So thank you for your testimony. I read your testimony, and I concur in a lot of the subjects that you brought up there, so thank you for coming today.

Mr. Chairman, thank you.

Senator SMITH. Thank you Senator Burns.

Senator Allen.

Senator ALLEN. Thank you Mr. Chairman, four different things, trying to get some clarification here. One is authority, second is resources, third is penalties, and fourth is what jurisdiction or standards we should be applying. Insofar as authority, and I'll ask you some questions, it seems like you have all the authority you need. Resources, you say you don't need more, but you—then on authority, the area that you need it more in, is not necessarily domestic but international. Resources you say you have enough, penalties, you need stronger penalties, particularly civil penalty standards. The question is whether you have 50 or 40 different standards, or a standard for all the United States and its territories. Now has there ever been a situation where the FTC could not bring a case

because you don't have sufficient authority under existing laws, other than, aside from the U.S. SAFE WEB Act, which is incorporated in part, and this is Senator Smith's measure. Is there any new authority that the FTC needs if you find in other words that somebody regardless of what their doing, if it's fraudulent and deceptive you can prosecute them, if it is misleading, if it is false and so forth. Has there ever been a situation where you didn't have the legal authority to prosecute within the United States?

Ms. MAJORAS. With respect to spyware, I'm not aware of any, no.

Senator ALLEN. So you feel that other than internationally, but within these orders of the United States, and our territories, you feel the FTC has the authority regardless of what the technology or method of deception is utilized?

Ms. MAJORAS. Well, we've successfully brought cases, we've got more in the pipeline. So that's correct. Other than what I've said about civil penalty authority, yes.

Senator ALLEN. What you do want is you want more civil authority. Civil penalties, I guess you could call that authority as well.

Ms. MAJORAS. We think that could be very helpful.

Senator ALLEN. And that's included in the measure the Chairman and I have introduced. Now if the Congress codified prescriptive definitions of illegal behavior that are specific to current technology, could we run the risk that this law could be obsolete as new technology continues to develop.

In other words by defining a specific illegal behavior, are we creating loopholes for spyware purveyors who figure out ways to get around the law?

Ms. MAJORAS. Well, that is possible. I mean, obviously Section 5 of the FTC Act would still be in effect, so we would hope that there was something that [inaudible] cracks, but we'd be able to use our broad authority to go after them. But what we wouldn't want is for a court to say, well it's not on the list, so therefore, sorry FTC, you can't go after them. That's really our only reservation.

Senator ALLEN. Because in effect, you could end up with a safe harbor for those using these fraudulent deceptive practices if they're not on that list, the court could say, well they're not on the list, so therefore you cannot prosecute.

Ms. MAJORAS. It's possible, we can't say for sure that's how a court would interpret it.

Senator ALLEN. Now so far, on the issue of jurisdiction, in the standard, so far 18 states have enacted legislation regarding spyware and many new laws are pending in several states. Since spyware, clearly by its nature is national, in fact it's international in its scope. Do you agree that a national framework is necessary to ensure a patchwork of state laws do not unnecessarily confuse and burden consumers and legitimate software providers?

Ms. MAJORAS. I think it's possible, depending on the differences among the various state laws that—probably consumers, less so—but that those who are actually trying to comply with the law. I mean they simply can't in the Internet context comply with multiple standards. I mean basically they would have to figure out what the highest standard is, I believe, and then comply with that one. And so—and if that weren't the Federal, if there are Federal standards, and that ends up not being the highest one, then I sup-

pose whichever state had the highest standard would become the de facto standard for the Nation.

Senator ALLEN. Well, for your enforcement would it not be best to have a—the best standard, the strongest standard, the most effective standard that's set for the Nation by the Federal Government and Congress?

Ms. MAJORAS. Well, I think a consistent standard would help all of us. And the fact of the matter is the state attorneys general are critical partners to us in this fight, but if we're all singing from the same hymn book sort of speak, I think we can be very effective.

Senator ALLEN. Well, our measure does have the attorneys general of the states involved, with a national standard, but have them helping enforce it, because in some cases the Federal Government can't do it all.

Ms. MAJORAS. That's exactly right. We would want the states to absolutely have authority.

Senator ALLEN. All right. Now on the questions of notice, and the notice and consent regime. According to this July 2005 Pew Internet and American Life Project, 73 percent they found according to them, 73 percent of Internet users do not always read user agreements, privacy statements, or other disclaimers, before downloading, or installing programs. There are some of us who will click through things real quickly because you want to read something. In fact, one study of a user agreement included a clause that promised $1,000 to the first person to write in and request that $1,000. The agreement was downloaded more than 3,000 times before somebody finally read the fine print and claimed the reward. Now do you believe that subjecting the entire software industry to a new notice and consent regime will help combat spyware?

Ms. MAJORAS. Overall, no, I don't think that would be the most effective tool. Our experience, while I don't have statistics, comports very closely with the conclusion of that survey. And that is, for better or for worse, consumers don't read these disclosures, and the more they are bombarded with similar disclosures, the less likely they are to read them. And what our concern has been is that we could have a spyware distributor who is distributing spyware that is very, very harmful to consumers, but then can just say, well I disclosed it to consumers that this is what I was going to do, so too bad for them. And while that has, no question, sensational appeal, because none of us want to be extraordinarily paternalistic to American consumers. When we know that they don't read these disclosures when they're downloading software, it makes it hard to say that's what we think would truly, would truly protect consumers.

What we're doing in our casework, is looking at disclosures on a case-by-case basis to see if we think they're adequate.

Senator ALLEN. Thank you, Mr. Chairman.

Senator SMITH. Thank you, Senator Allen.

Senator ALLEN. Thank you, Madam Chairman.

Senator SMITH. To Senator Allen's point and your answer, that you today announced the Odysseus case that you're pursuing, and is this not a company that offers through peer-to-peer enticements to children, free music and other things that they readily go past

the disclosures to get what's free, but in the end it's maybe very promotional, and a very degrading thing?

Ms. MAJORAS. It's similar, they were working in the peer-to-peer realm. And the representation they made was that by downloading their software, your peer-to-peer presence would be anonymous and no one would be able to trace you. That, we alleged, isn't true. And then, in addition, they've downloaded a lot of other software, which in essence as we say in the complaint, just to summarize it here, hijacks the consumer's computer.

Senator SMITH. Isn't that already illegal?

Ms. MAJORAS. Yes. We've filed a suit under Section 5 of the FTC Act.

Senator SMITH. Do you think you'll win, if it's already illegal? Because I want to make sure it's illegal.

[Laughter.]

Ms. MAJORAS. Well, I certainly understand that Senator, and I can't—I couldn't tell you that nobody would ever challenge our authority or that a judge would never—you know could never find that we didn't have such authority, but it's not been a problem to date. And we feel that this isn't a close call under Section 5 of the FTC Act and so we brought the case.

Senator SMITH. So the people who are maybe here, or interested in it. I understand that the software actually changes your search results that consumers get from search engines, like Google and Yahoo, and that this is done without the consumers knowledge.

Ms. MAJORAS. That's exactly right. I mean we don't think that they have a way necessarily of knowing. So as you know it's important to some, to be the first in a Google search results, or what have you, and this apparently can change the results around, but again, no, the consumers wouldn't necessarily know that was even happening to them.

Senator SMITH. Well, if you find out it isn't illegal, let us know.

Ms. MAJORAS. You would be the first call we would make.

Senator SMITH. I mean our bill does address this very kind of thing. And so you know, that's why we keep asking you if you need any more resources, do you need more authorities? Because this really gets to the heart of what we're trying to accomplish for the protection of American consumers without stifling innovation in future technologies. Do you see a way? I mean you've heard all of us up here, all agreeing there's a problem we want to fix, and the difference and the difficulty is in the breadth of how we would go about it. I guess as you evaluate the two different bills that are represented here, is there a way to merge them in your mind?

Ms. MAJORAS. Well, I think there's probably, there probably is a way to bring it together and one—I mean if we could classify them, your bill restates the FTC's authority to attack software, but in a more general way. The other bill tries to be a bit more specific about it. And I would just caution that if specifics are going to be added to any legislation that becomes law that it is made absolutely clear that other types of conduct may also be illegal, within this same family and that the FTC's authority is not being narrowed by this.

Senator SMITH. And if we leave it broad, to the degree you need to make it narrower, do you have rulemaking authorities to make it narrower?

Ms. MAJORAS. Well, we would have rulemaking authority if you gave it to us, if it was needed. The one area where I think it's difficult to reconcile is with respect to notice. Which again I agree has very—has facial appeal, it does to me too, but I just don't—our experience is it doesn't actually protect consumers. And since that's our job, it's hard for me to support that.

Senator SMITH. And there's a lot of advertising that is actually promoting very valuable things, and useful products and we don't want to get in the way of that.

Ms. MAJORAS. No. No, we don't want to get in the way of it, and in fact there may be First Amendment issues if we tried to go too far.

Senator SMITH. As I understand the U.S. SAFE WEB Act which you have indicated your support for, its provisions are really not all that new or unusual, there are other agencies in the government that already have these powers, is that your understanding?

Ms. MAJORAS. Absolutely. The SEC, the CFTC, and banking agencies.

Senator SMITH. You need them too?

Ms. MAJORAS. We do, I can't emphasize it enough Chairman Smith.

Senator SMITH. Well, Chairwoman Majoras, thank you very much. Yes, please.

Senator ALLEN. My time has expired but may ask some questions.

Senator SMITH. Yes, please go ahead.

Senator ALLEN. I just want to follow up on your good probative questions. Your caution trying to figure these things out, several things that you asked for, you asked for the international authority, the U.S. SAFE WEB Act, that's part of our measure, it is not part of Senator Burns' measures. So that was one thing where you wanted regular authority. That probably can be merged together. We do have a fundamental difference on the jurisdiction and how you define illegal behavior, which right now is very broad. If it's fraudulent or deceptive, if it's misleading, you know, it's illegal which is what you'd want. You could limit yourself by prosecutorial discretion I suppose, and in a court the trier of fact would say, well no that isn't deceptive. As opposed to specifying a bunch of different specific illegal methods, which could end up with a safe harbor if it's not on that list. And maybe the solution to that, is to say well these are illegal but they are not the only ones that are illegal. Anything is, but then the other side feels like all right, we've at least specified these. I suppose that could be worked out. The notice issue is one that I do think is irreconcilable. Because as I was—there was a reason I asked that question, and why some 3,000 hits are getting $3,000. Folks just simply don't read it, they don't have time for it. Even looking on this—who's going to go through—now I think it's helpful for those in the IT departments of companies, somebody's going through all that, and seeing which are good spyware blocker programs. But a normal person in their home is just generally not going to go through all that. So there

does need to be a better business bureau approach. And I see that's what that is. Now you get into the issue of jurisdiction. That's a key one as to whether you have a national standard, or 50 or 40 different states standards. I think to make companies to have to comply with 40 different standards, and maybe different nuances and different case law and all the rest makes it very difficult. To me that is not irreconcilable difference. Now I think it's important to respect the rights, and prerogatives of the states, and prosecution and that's why in our measure we do have the attorneys general brought in.

You wanted also the civil fines, which will be helpful. The one thing I find interesting though was your answer on the question of, you don't need any more resources. Here's my perspective of that. Is that this is so pervasive and you have nearly 50 percent of all computers being hit with this spyware, and it's great that you've brought these big cases, and you've knocked down organizations, spyware organizations and you say how difficult it is to prosecute and find these people, well if you're dealing with normal criminal behavior and you have a certain amount of resources, if you actually had more detectives so to speak, more investigators, more funds if there were drug dealing for undercover agents, or making drug buys, or—those resources do matter in combating illegal drug activity.

So I find it interesting that you say that you don't need any more resources when this is such a big pervasive problem of this fraudulent and deceptive activity. If you have the civil penalties and I don't know the answer to this, but where do the fines, if fines are—does that go to the general fund, or does that go—would that go to further law enforcement efforts?

Ms. MAJORAS. I believe it goes to the general fund, yes. It goes into the Treasury. It goes into the Treasury.

Senator ALLEN. All right. In drug dealing, with asset forfeiture, for those assets that are traceable to illegal drug dealing, that actually goes Mr. Chairman to law enforcement so that they use it for undercover drug buys, paying overtime, surveillance costs, sometimes paying informants for example, it's like catching the shark and cutting it up for bait. Use the assets to catch more sharks. Why do you say that you don't need more resources with—and maybe this is what the Administration wants you to say and I understand that, having been a Governor, I expected all my agency heads to tow the line. But with something that is so pervasive, and obviously of bipartisan concern, and not just us, but obviously to the American people and to the technology community generally and the Internet, why would it not be helpful for you to have more personnel to actually get after this obviously growing, disruptive, illegal behavior?

Ms. MAJORAS. Well, I appreciate the question and, no, Senator, nobody's asked me to tow any line on this. You know we've actually been very pleased. We think as other agencies have been cut back in the last couple of years, as some belts have been tightened, we think that Congress has been very generous with us, which we appreciate and that they recognize the importance of our work.

Look, if you give us more resources, we'll——

Senator ALLEN. What would you do with them?

Ms. MAJORAS.—certainly use them. Well, probably one of the things I would do, is I would hire some more tech experts, who can help us with some of the difficulties in actually hunting down these folks, or in helping us find ways to push industry in the right direction. Because I do think that ultimately technology will—is what will help us prevail. So I think we can. But the only issue I would say with respect to having a very large amount of new funds, which are actually earmarked for a particular purpose, is that what tends to happen is then if priorities shift and change, because for example new spyware tools come out and that tends to be less a problem, and the bad guys, if you will, have moved on to something else, then we have to come back to you and say, look we have this pot of money, which you wanted us to use for this purpose, but quite frankly priorities have changed, and they would have even changed for you. And so that's part of something that we obviously would have to work with you on, Senator.

But obviously our job is to enforce the laws that Congress passes and to take our lead from consumers first, and obviously you are the elected representatives who represent them. So if you want us to have more resources to send the message to us that I've got to put more investigators on this, then obviously we will do that.

Senator ALLEN. Well, in the event you actually solve this problem quickly, obviously appropriations are annual. Even if appropriations actually get done in a timely manner, I suspect that the fines and forfeitures that you will glean from these added—not that the law enforcement is simply to gain money for the government, but I suspect with greater enforcement not only will you have the Internet being more useful and less aggravating and less—fewer computers shut down because they're clogged up with all of this spyware, is that you'll actually end up getting more fines and forfeitures, and assets seized than that $10 million over the period of this measure. And if you didn't need the money, you can always say, we need it more for something else. But I don't see this getting solved in the next few years. I think it could be ameliorated, I think it could be mitigated, but this is—it's too lucrative a business, illegal enterprise right now, and to the extent you drive it out of this country, you're still going to have it overseas, and that's why the U.S. SAFE WEB Act is so important and have the international community caring as much about this as we try to get the international community to care about intellectual property rights for example.

Ms. MAJORAS. That's right.

Senator ALLEN. To the extent you ever get it to that point, fine, we'll save some money there. And you're doing a great job, and you've had some good noteworthy cases, but you also recognize that it's just the tip of the iceberg in this illegal spyware enterprise.

Ms. MAJORAS. Indeed, not only do we recognize it, but we would hate to raise expectations way too high, because we're going to keep at this. I mean, you know, we talk all the time about how the worst thing that could happen to us would be for our consumers to just simply lose faith in this wonderful new medium that we have that is the Internet. And we can't let that happen, and we have to—we really have to guard and protect consumer's confidence in it. So we're going to keep at it. But I point out the difficulties

in tracking these folks down and so forth, only to remind us again that it won't be just law enforcement that's going to tackle this problem, we need new technology.

And the good news is, that if we do get these additional international resources, we can leverage that. We spend a lot of resources trying to chase down people in countries where we're trying to hire lawyers who know what they're doing over there when we don't, and so on and so forth, and we could use our counterparts and vice versa, then we will be actually a lot more efficient even in our use of resources.

So I appreciate your point Senator Allen.

Senator ALLEN. Well, thank you. And thank you, Mr. Chairman, just understand Madam Chairman that the Chairman here and this Senator want to work with you and do this effectively. And we do feel that you need out of jurisdiction as you say, or added authority. And I do feel that you do need more resources to get the job done, and it shouldn't just be the government, it does need to be the technology industry. They are the ones who are the most creative in coming up with the firewalls, and the filters, and the ways to block unwanted spyware, or illegal spyware. There is some spyware which has—and you were very clever answering those questions of Senator Nelson. But you know in some cases it's not harmful, it's not deceptive and so forth. I do think it's going to take a concerted team effort on the part of the technology community and actually probably can—I just have faith in their innovative, creative capabilities to make sure the Internet stays a great invention for the dissemination of information and ideas, and commerce, and education, and tele-medicine, and in so many ways, improving our lives in commerce. So I thank you again Mr. Chairman for your leadership, look forward to working with you, and Madam Chairman, thank you for articulate principled leadership.

Ms. MAJORAS. Thank you very much, Senator Allen.

Senator SMITH. And Madam Chairman, to Senator Allen's point, I think if you hear anything today it is that this is an enormous problem and it requires urgent effort, and so please know we're counting on you, we appreciate you, and we hope you convey to everyone at the FTC we appreciate their good work. We recognize in our mailboxes that there is growing alarm and we need to be ahead of it. So thank you, and with that we're adjourned.

Ms. MAJORAS. Thank you very much, Senator.

[Whereupon, at 3:40 p.m., the Committee adjourned.]

A P P E N D I X

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK R. LAUTENBERG TO HON. DEBORAH P. MAJORAS

Response to Questions One and Three

Your letter poses two questions about the nature and efficacy of the FTC's consumer education efforts related to spyware. Your letter commends the FTC and industry for launching a new website, *www.OnGuardOnline.gov*., but expresses the concern that the website uses technical terms (e.g., updating operating systems, firewalls, and drive-by installations) that consumers, particularly seniors, may not understand. Your letter also cites statistics as to the prevalence of spyware on computers and asks about the Commission's short-term and long-term goals to decrease its prevalence through consumer education.

The Commission shares your concern about the importance of educating consumers about problems in electronic commerce, including spyware. To inform consumers about spyware and other threats on the Internet, the Commission launched its OnGuard Online initiative, with the OnGuardOnline.gov website as its primary consumer education tool. The initiative was developed to address the need for a comprehensive, consistent set of educational messages for consumers. It incorporates the best learning of the Internet community and presents it in a complete and accessible format. In consultation with communications experts, it was designed to be usable by consumers with a broad range of familiarity with the Internet and technology. The comprehensive website uses interactive activities, articles, videos, and tips that address topics important to consumers, including ways that consumers can lower their risk of spyware infections, clues as to whether spyware is on their computer, and an informative spyware quiz. Consumers are also able to report via the website if they have been a victim of spyware.

Because people learn in a variety of ways, the FTC has made the OnGuard Online information available in many forms. The OnGuardOnline.gov website includes video tutorials prepared by the Internet Education Foundation with visual instructions to "click here, then here," to turn on the security features in various types of software. The site also presents a series of videos prepared by Microsoft with the information presented in an accessible format.

Some consumers, including many seniors, may not be familiar with technical terms used to describe technology. The OnGuard Online initiative therefore uses plain language to describe technical concepts. For example, the OnGuard Online brochure explains that "[f]irewalls help keep hackers from using your computer to send out your personal information without your permission." In addition, the OnGuard Online bookmarks and posters have quick tips written in plain language, and the OnguardOnline.gov website includes an extensive glossary of computing terms, for consumers who need more information about the terms used. Finally, the AARP is a partner in the OnGuard Online initiative.

Response to Question Two

Your letter asks whether it is deceptive to fail to disclose that spyware will be installed. Your letter also asks whether it is deceptive to disclose only in the end-user license agreement that spyware will be installed.

It is well-established that a failure to disclose adequately material facts to consumers may be unfair or deceptive in violation of Section 5 of the FTC Act. The FTC has alleged a failure to disclose information in a number of Internet-related deception cases. [1] The Commission staff also has issued a guidance document that pro-

[1] *See, e.g., Juno Online Services, Inc*., FTC Dkt. No. C–4016 (June 29, 2001) (failure to disclose that some subscribers to its ISP service would incur long distance telephone charges while connecting to the Internet) (consent order); *BUY.COM, Inc*., FTC Dkt. No. C–3978 (Sept. 8, 2000) (failure to disclose restrictions and costs associated with purchasing a "free" or "low-cost" per-

Continued

vides advertisers with advice as to how to apply traditional FTC disclosure principles to the online environment, including advertising and marketing software on the Internet.[2]

The Commission has addressed the failure to disclose adequately to consumers the material fact that spyware would be installed on their computers. In particular, disclosing the presence of bundled software, including spyware, only in the end-user licensing agreement may be unfair or deceptive. For example, in *FTC* v. *Odysseus Marketing, Inc.,* the defendants offered consumers a free software program that purported to make the consumers anonymous when using peer-to-peer file-sharing programs.[3] The Commission alleged, however, that the distributors failed to disclose to consumers that this program, in turn, would install other, harmful software on their computers. Similarly, in *Advertising.com, Inc.,* the respondents allegedly offered free security software, but bundled with it software that caused consumers to receive a substantial number of pop-up ads.[4] Although the presence of this software was disclosed in the end-user license agreement, the Commission alleged that this disclosure was inadequate. The Commission therefore is using its authority to prohibit unfair or deceptive acts and practices to take law enforcement action against those who fail to disclose adequately to consumers that spyware will be installed on their computers. It is important to note that, as I indicated in my testimony, such a case-by-case approach that focuses on bringing law enforcement action where a failure to disclose has harmed consumers is preferable to requiring disclosure for all software, no matter how innocuous.

Response to Question Four

As the Commission indicated in its testimony,[5] our main tool for combating spyware is bringing law enforcement actions challenging acts and practices as unfair or deceptive in violation of Section 5 of the FTC Act. Your letter asks how many spyware-related law enforcement actions we have brought in 2005, as well as for a description of our efforts to investigate spyware, given that many consumers may not know that they have spyware on their computers.

Thus far, the FTC has brought six law enforcement actions involving spyware, including five law enforcement actions to date in 2005. The FTC's written testimony at the recent hearing describes the FTC's first five actions. Our sixth law enforcement action was filed after the hearing.[6] In the *Enternet Media, Inc.* case, the FTC alleged that the defendants distributed via the Internet exploitive software code dubbed "Search Miracle" and "EliteBar," onto the computers of unsuspecting consumers. With the aid of their network of affiliates, the complaint alleged, the defendants trick consumers into downloading and installing their exploitive code by disguising it as harmless, free software, such as Internet browser upgrades, music files, cell phone ring tones, and song lyrics. However, contrary to their representations, the defendants' code is not a browser upgrade or security patch, nor is it any type of harmless free software. Rather, it functions as a type of spyware that substantially interferes with the functionality of consumers' computers, such as by tracking consumers' Internet activity, changing consumers' homepage settings, inserting a new toolbar onto consumers' Internet browsers, inserting an obtrusive window onto consumers' computer screens that displays advertisements, and displaying voluminous pop-up advertisements, even when consumers' Internet browsers are closed. To make matters worse, the FTC alleges, it is extremely difficult for consumers to uninstall the exploitive code, and that the defendants' uninstall instructions do not work. A Federal district court granted a temporary restraining order; a preliminary injunction hearing has been scheduled for the near future. Using this

---

sonal computer in exchange for agreeing to purchase Internet service) (consent order); *Value America, Inc*., FTC Dkt. No. C–3976 (Sept. 8, 2000) (same).

[2] Federal Trade Commission Staff Working Paper, Dot Com Disclosures: Information About Online Advertising (May 3, 2000), available at *http://www.ftc.gov/bcp/conline/pubs/buspubs/dotcom/index.html*.

[3] The Commission recently filed a complaint in Federal court alleging that this failure to disclose was deceptive in violation of Section 5 of the FTC Act. The parties stipulated to a preliminary injunction order, which was entered on October 11, 2005. *FTC* v. *Odysseus Marketing, Inc*., No. 05–CV–330 (D.N.H. filed Sept. 21, 2005), available at *http://www.ftc.gov/opa/2005/10/odysseus.htm*.

[4] *In the Matter of Advertising.com*, FTC Dkt. No. C–4147 (consent order Sept. 12, 2005), available at *http://www.ftc.gov/os/caselist/0423196/0423196.htm*.

[5] Federal Trade Commission, *Prepared Statement Before the Committee on Commerce, Science, and Transportation Subcommittee on Trade, Tourism, and Economic Development, United States Senate* (Oct. 5, 2005), available at *http://www.ftc.aov/os/testimonv/051005spywaretest.pdf*.

[6] *FTC* v. *Enternet Media, Inc*., No. CV–05–7777 (C.D. Cal. filed Nov. 1, 2005).

law enforcement approach, we were also able to freeze $2 million in the defendants' bank accounts.

Spyware investigations and prosecutions are a priority for the Commission. We are actively looking at a wide variety of sources of information about the identity and location of those distributing spyware that is causing harm to American consumers. We are consulting with Federal and state criminal and civil law enforcement agencies. We also are receiving critical information from high-tech companies, such as anti-spyware companies and operating system companies. We further are receiving valuable information from consumer groups, anti-spyware organization websites, academics, and the technology press. I appreciate the assistance that we are receiving from these groups, and I look forward to continue working with them to make our spyware investigations and prosecutions as effective as possible.

Thank you for providing me with an opportunity to supplement my answers at the hearing concerning the FTC's law enforcement record as it pertains to spyware. If you would like additional information, please contact Anna Davis, the Director of the Office of Congressional Relations, at (202) 326–3680.