

**IMPACT AND POLICY IMPLICATIONS OF
SPYWARE ON CONSUMERS AND BUSINESSES**

HEARING

BEFORE THE

**COMMITTEE ON COMMERCE,
SCIENCE, AND TRANSPORTATION**

UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

—————
JUNE 11, 2008
—————

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



U.S. GOVERNMENT PRINTING OFFICE

76-328 PDF

WASHINGTON : 2012

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

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

DANIEL K. INOUE, Hawaii, *Chairman*

JOHN D. ROCKEFELLER IV, West Virginia	TED STEVENS, Alaska, <i>Vice Chairman</i>
JOHN F. KERRY, Massachusetts	JOHN McCAIN, Arizona
BYRON L. DORGAN, North Dakota	KAY BAILEY HUTCHISON, Texas
BARBARA BOXER, California	OLYMPIA J. SNOWE, Maine
BILL NELSON, Florida	GORDON H. SMITH, Oregon
MARIA CANTWELL, Washington	JOHN ENSIGN, Nevada
FRANK R. LAUTENBERG, New Jersey	JOHN E. SUNUNU, New Hampshire
MARK PRYOR, Arkansas	JIM DEMINT, South Carolina
THOMAS R. CARPER, Delaware	DAVID VITTER, Louisiana
CLAIRE McCASKILL, Missouri	JOHN THUNE, South Dakota
AMY KLOBUCHAR, Minnesota	ROGER F. WICKER, Mississippi

MARGARET L. CUMMISKY, *Democratic Staff Director and Chief Counsel*

LILA HARPER HELMS, *Democratic Deputy Staff Director and Policy Director*

CHRISTINE D. KURTH, *Republican Staff Director and General Counsel*

PAUL NAGLE, *Republican Chief Counsel*

CONTENTS

	Page
Hearing held on June 11, 2008	1
Statement of Senator Nelson	2
Statement of Senator Pryor	1
Statement of Senator Vitter	2

WITNESSES

Butler, Arthur A., Attorney, Ater Wynne LLP, on behalf of Americans for Fair Electronic Commerce Transactions (AFFECT)	12
Prepared statement	13
Cerasale, Jerry, Senior Vice President, Government Affairs, Direct Marketing Association, Inc.	16
Prepared statement	18
Edelman, Benjamin G., Assistant Professor, Business Administration, Harvard Business School	29
Prepared statement	31
Harrington, Eileen, Deputy Director, Bureau of Consumer Protection, Federal Trade Commission	3
Prepared statement	4
Rotenberg, Marc, Executive Director, Electronic Privacy Information Center (EPIC)	23
Prepared statement	24
Weafer, Vincent, Vice President, Security Response, Symantec Corporation, on behalf of the Business Software Alliance (BSA)	35
Prepared statement	36

APPENDIX

Letter dated June 24, 2008, from John P. Tomaszewski, Esq., Vice President, Legal, Policy and Compliance, TRUSTe, to Hon. Mark Pryor	49
Letter dated June 25, 2008, to Hon. Mark Pryor from Arthur A. Butler, Attorney, Ater Wynne LLP; on behalf of Americans for Fair Electronic Commerce Transactions (AFFECT)	52
Response to written questions submitted by Hon. David Vitter to Eileen Harrington	55

IMPACT AND POLICY IMPLICATIONS OF SPYWARE ON CONSUMERS AND BUSINESSES

WEDNESDAY, JUNE 11, 2008

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

The Committee met, pursuant to notice, at 3:07 p.m. in room SR-253, Russell Senate Office Building, Hon. Mark Pryor, presiding.

OPENING STATEMENT OF HON. MARK PRYOR, U.S. SENATOR FROM ARKANSAS

Senator PRYOR. Someone out there told me, don't start being like the airlines, being late on everything. So we won't do that. I'm sorry that I was a few minutes late, but I got caught in a previous meeting.

I want to thank Chairman Inouye and Vice Chairman Stevens for holding this hearing to review the efforts by industry, the Federal Trade Commission, and Congress, to combat spyware and its effects on consumers. Specifically, this hearing will look at the impact of spyware on computer performance, along with privacy and security risks associated with this software.

In particular, the hearing will consider a bill that I filed, S. 1625, the Counter Spy Act, and that I introduced with Senator Bill Nelson and Senator Boxer. Also, just to let other Senators and other staff know, we thought we'd have this hearing and sit down with our bill and see if we can get some other cosponsors and help us think through some issues there. So I want to thank all the witnesses today for being part of that process.

Spyware is a pervasive problem that really I believe demands swift action by Congress to protect American consumers from very significant privacy and security risks. There are very few, if any that I can determine, legitimate reasons for this practice of having spyware in the first place, and there are numbers of reasons why we should do something to try to stop spyware.

Basically, I think our bill needs to do two very important things. One is we need a good workable definition of spyware. It's hard to define, but we need to come up with a Federal definition where there's a standard.

The second thing is we need to come up with some civil penalties in the event that someone is out there using spyware in an unauthorized manner. We need to have a civil penalty regime so that the FTC knows exactly what they need to do and what steps they need to take.

I guess the other part that's kind of implicit in both of those is that we need to make sure that whatever we pass is very consumer-friendly, so consumers know that when spyware is present on their system or asking to be loaded or whatever the case may be, that the consumers have a chance to stop it from being added to their computers in the first place.

So with that, what I would like to do is ask Senator Vitter if you have an opening statement.

**STATEMENT OF HON. DAVID VITTER,
U.S. SENATOR FROM LOUISIANA**

Senator VITTER. Thank you, Mr. Chairman. I'll be very brief. Thank you for this hearing. This is an extremely important topic. I agree with you that it's a really serious problem that we should move absolutely as quickly as possible to address. I certainly want to be part of the discussions and the solution.

That's the easy part. The tough part is how we do that effectively. I think the biggest challenge in so many of these issues is to come up with legislation that isn't outpaced or becomes outdated by technology in a month or a year. So I believe we should focus on passing legislation against improper activity and not be too technologically specific, because I think that's going to end up getting us in trouble, having unintended consequences, or just being outdated relatively soon.

So I'm very interested in legislation. Some of the things I want to avoid is to enact things that would be technology mandates, to enact things that might unintentionally hamper the ability of the FTC and law enforcement to adopt a technology and that could be interpreted so broadly that it would extend beyond unwanted spyware to affect all web pages or to affect online transactions that folks do want and get some convenience out of.

So thank you again for this hearing. I look forward to hearing from the witnesses and asking questions with the goal of helping develop that sort of bipartisan legislation.

Senator PRYOR. Thank you.

Senator Nelson, I'll call on you for an opening statement if you'd like to make one and then ask you to introduce the first witness.

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

Senator NELSON. Mr. Chairman, you have to go back to a conference committee?

Senator PRYOR. Yes.

Senator NELSON. So I will await your return.

Senator PRYOR. Thank you.

Senator NELSON [presiding]. *Consumer Reports* in a recent edition had a survey and of the 2,000 people surveyed, one in eleven reported a major spyware infection on their computer. These infections are costly, may well cost over \$100 to fix, and the overall calculated impact on the economy is \$1.7 billion. That's a figure that's only going to increase.

So that's why we filed this legislation. We also hope that the Federal Trade Commission and other law enforcement agencies are

going to take further action to pursue to the maximum extent possible foreign spyware developers.

Now, in another arena, in the intelligence arena, in the defense arena, we have a particular concern which is not the subject of the discussion here today. But clearly that overlays the problem that we're talking about on consumers today.

So we are delighted to have Ms. Eileen Harrington, Deputy Director of the Bureau of Consumer Protection at the FTC. So, Ms. Harrington, your presentation, please. Your lengthy statement will be a part of the record, so if you would just summarize, and then we'll get right into the questions. Thank you.

**STATEMENT OF EILEEN HARRINGTON, DEPUTY DIRECTOR,
BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE
COMMISSION**

Ms. HARRINGTON. Thank you very much, Senator Nelson and Chairman Pryor and Members of the Committee. I am Eileen Harrington.

Spyware and other malware causes substantial harm to consumers and to the Internet as a medium of communication and commerce. Protecting consumers from this harm is a priority for the Federal Trade Commission and we thank you for giving us the opportunity to appear here today to talk about the FTC's activity in this area and to comment on S. 1625, the Counter Spy Act, which was introduced by Senator Pryor, Senator Boxer, and Senator Nelson.

Since 2004 the FTC has brought 11 spyware-related law enforcement actions and, while we certainly haven't solved the spyware problem, our law enforcement efforts have, we believe, had an effect and have reduced the prevalence of pop-up ads generated by nuisance adware. Our spyware law enforcement actions reaffirmed three key principles.

The first is that a consumer's computer belongs to him or her, not to the software distributor, and it must be the consumer's choice whether or not to install software. This principle reflects the basic common sense notion that Internet businesses are not free to help themselves to the resources of a consumer's computer.

The second principle articulated in our enforcement work is that buried disclosures of material information necessary to correct an otherwise misleading impression are not sufficient, just as they have never been sufficient in more traditional areas of commerce. Specifically, burying material information in an End User License Agreement will not shield a spyware purveyor from Section 5 liability.

The third principle underscored by our work is that if a distributor puts a program on a computer that the consumer does not want the consumer should be able to uninstall or disable it.

As in so many other areas, cooperation among law enforcement agencies is vital to successful enforcement in the spyware area. Many of the worst abuses connected with spyware are criminal activity in nature and we at the FTC coordinate very closely with our colleagues at the Department of Justice to see to it that these criminals are prosecuted. The FTC also coordinates closely with

State law enforcement partners who bring enforcement actions against spyware distributors.

Now, in addition to engaging in law enforcement and coordinating with others in the enforcement community, the FTC has made consumer education a priority. In September 2005, the FTC formed a partnership with other Federal agencies in the technology industry to launch a multimedia interactive consumer education initiative, OnGuard Online. The *OnguardOnline.gov* website now attracts over 350,000 unique visits each month and many organizations have taken the OnGuard Online materials for their own security training. The comprehensive website has general information on online safety as well as sections with specific information on a range of topics, including spyware.

Turning to the bill under discussion, S. 1625, we would make two points. First, although we have successfully used Section 5 of the FTC Act to challenge conduct related to spyware distribution under Section 5, legislation authorizing the Commission to seek civil penalties in spyware cases would provide a welcome addition to remedies available to us. Currently under Section 13(b) of the FTC Act we have authority to file actions in Federal district court and to obtain injunctive and equitable monetary relief in the form of consumer redress or disgorgement. In spyware cases, however, restitution or disgorgement may be neither appropriate nor sufficient remedies because consumers often have not purchased a product or a service from the defendants, the harm to consumers may be very difficult to quantify, or the defendant's profits may be slim or difficult to calculate with certainty. In such cases a civil penalty may be a far better remedy and serve as a stronger deterrent.

Second, under general consumer protection principles and traditional Section 5 jurisprudence, the Commission need not show knowledge or intent in order to obtain injunctive relief, but several sections of S. 1625 impose an overarching knowledge or intent threshold for enforcement that could create a higher and more difficult evidentiary burden for the FTC in obtaining injunctions in civil spyware cases.

Section 5(m)(1) of the FTC Act already requires that the Commission prove knowledge in any civil penalty action. Eliminating the knowledge or intent threshold from S. 1625 would not change the Commission's elevated burden regarding civil penalties, but it would maintain the ordinary burden that we have to meet in order to obtain injunctive relief. So we would recommend that change.

I thank you for focusing your attention on this important issue and giving us the opportunity to discuss the Commission's enforcement record. Thank you.

[The prepared statement of Ms. Harrington follows:]

PREPARED STATEMENT OF EILEEN HARRINGTON, DEPUTY DIRECTOR,
BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

I. Introduction

Chairman Pryor and members of the Committee on Commerce, Science, and Transportation, I am Eileen Harrington, Deputy Director of the Bureau of Con-

sumer Protection of the Federal Trade Commission (“Commission” or “FTC”).¹ Spyware and other malware can cause substantial harm to consumers and to the Internet as a medium of communication and commerce. Protecting consumers from such harm is a priority for the Commission, and the agency thanks this Committee for the opportunity to describe what the FTC is doing in this area and to provide input on S. 1625, the “Counter Spy Act” introduced by Senators Pryor, Boxer, and Nelson.

This written statement provides background on the Commission’s active program to address concerns about spyware and other malware, which includes law enforcement actions and consumer education efforts. First, it discusses the Commission’s three key principles related to spyware as illustrated by the eleven spyware-related law enforcement actions the agency has initiated to date. Second, the statement highlights the Commission’s consumer education efforts on spyware. Third, the statement offers the Commission’s views on the proposed legislation, S. 1625.

The Commission has a broad mandate to prevent unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.² Although it is often challenging to locate and apprehend the perpetrators, the FTC has successfully challenged the distribution of spyware that causes injury to consumers online.

Spyware and other malware that is downloaded without authorization can cause a range of problems for computer users, from nuisance adware that delivers pop-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 law enforcement and consumer education. Since 2004, the Commission has initiated eleven spyware-related law enforcement actions.³ While the problem of spyware has not been solved, our cases have had a significant effect and, based on our investigative experience, we believe the prevalence of pop-up ads generated by nuisance adware has been dramatically reduced.

II. Spyware Law Enforcement

A. FTC Cases

The Commission’s spyware law enforcement actions reaffirm three key principles. The first is that a consumer’s computer belongs to him or her, not to the software distributor, and it must be the consumer’s choice whether or not to install software. This principle reflects the basic common-sense notion that Internet businesses are not free to help themselves to the resources of a consumer’s computer. For example, in *FTC v. Seismic Entertainment Inc.*,⁴ and *FTC v. Enternet Media, Inc.*,⁵ the Commission alleged that the defendants unfairly downloaded spyware to users’ computers without the users’ knowledge, in violation of Section 5 of the FTC Act. Stipulated permanent injunctions were entered against the defendants in both matters, and defendants were ordered to disgorge more than \$6 million, combined.

The second principle is that buried disclosures of material information necessary to correct an otherwise misleading impression are not sufficient, just as they have never been sufficient in more traditional areas of commerce. Specifically, burying material information in an End User License Agreement will not shield a spyware purveyor from Section 5 liability. This principle was illustrated in *FTC v. Odysseus Marketing, Inc.*⁶ and *Advertising.com, Inc.*⁷ In these two cases, the Commission’s complaint alleged (among other violations) that the defendants failed to disclose adequately that the free software they were offering was bundled with harmful software programs. The orders entered in both cases require the defendants to disclose properly the effects of software programs that they offer in the future.

The third principle is that, if a distributor puts a program on a computer that the consumer does not want, the consumer should be able to uninstall or disable

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 Commissioner.

² 15 U.S.C. § 45.

³ Detailed information regarding each of these law enforcement actions is available at http://www.ftc.gov/bcp/edu/microsites/spyware/law_enfor.htm.

⁴ *FTC v. Seismic Entertainment, Inc.*, No. 04–377–JD, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Mar. 22, 2006), available at <http://www.ftc.gov/os/caselist/0423142/0423142.shtm>.

⁵ *FTC v. Enternet Media, Inc.*, CV 05–7777 CAS (C.D. Cal., Aug. 22, 2006), available at <http://www.ftc.gov/os/caselist/0523135/0523135.shtm>.

⁶ *FTC v. Odysseus Marketing, Inc.*, No. 05–CV–330 (D.N.H. Oct. 24, 2006) (stipulated permanent injunction), available at <http://www.ftc.gov/os/caselist/0423205/0423205.shtm>.

⁷ *In the Matter of Advertising.com, Inc.*, FTC Dkt. No. C–4147 (Sept. 12, 2005) (consent order), available at <http://www.ftc.gov/os/caselist/0423196/0423196.shtm>.

it. This principle is underscored by cases against Zango, Inc.⁸ and DirectRevenue LLC.⁹ These companies allegedly provided advertising programs, or adware, that monitored consumers' Internet use and displayed frequent, targeted pop-up ads—over 6.9 billion pop-ups by Zango alone. According to the Commission's complaints, the companies deliberately made these adware programs difficult for consumers to identify, locate, and remove from their computers, thus thwarting consumer efforts to end the intrusive pop-ups. Among other relief, the consent orders require Zango and DirectRevenue to provide a readily identifiable means to uninstall any adware that is installed in the future, as well as to disgorge \$3 million and \$1.5 million, respectively.

Similarly, in *FTC v. Digital Enterprises, Inc.*,¹⁰ the Commission alleged that the defendants installed software onto consumers' computers that repeatedly launched text and video pop-ups that consumers could not close or minimize. These pop-ups demanded payment for access to the defendants' purported entertainment websites. Among other relief, the September 2007 stipulated permanent injunction requires the defendants to provide a way for consumers to remove the software, bars future downloads without consumer consent, and requires the defendants to pay more than \$500,000 for consumer redress.

In addition, the agency's law enforcement efforts have alerted the Commission to novel spyware-related consumer protection issues such as the marketing of bogus anti-spyware programs. For example, in *FTC v. MaxTheater, Inc.*¹¹ and *FTC v. Trustsoft, Inc.*,¹² the FTC alleged that the defendants made false claims to consumers about the existence of spyware on their machines and then used these false claims to convince consumers to conduct free "scans" of their computers. These scans would identify innocuous software as spyware, helping to persuade consumers to purchase the defendants' spyware removal products at a cost of between \$30 and \$40. Moreover, the FTC alleged, the defendants claimed their spyware removal products could effectively uninstall many different types of known spyware programs, but the defendants' products did not perform as promised. In both cases, courts entered stipulated permanent injunctions prohibiting the claims and requiring the defendants to disgorge a total of nearly \$2 million.

B. Cooperation with Department of Justice and State Law Enforcement

As in so many other areas, cooperation among law enforcement agencies is vital to successful law enforcement in the spyware arena. Many of the worst abuses connected with spyware are criminal,¹³ and, in appropriate cases, the Commission coordinates closely with the Department of Justice. For example, in *FTC v. ERG Ventures, LLC*,¹⁴ the FTC's complaint alleged that the defendants secretly downloaded multiple malevolent software programs, including spyware, onto millions of computers without consumers' consent. The defendants also allegedly tricked consumers into downloading harmful software by hiding the malicious programs within seemingly innocuous free software. The U.S. Attorney's Office for the District of Columbia launched a parallel criminal investigation, and executed search warrants simultaneously with the filing of the FTC's civil case.¹⁵

The Commission also coordinates with state partners who bring their own law enforcement actions against spyware distributors. The FTC has established a Federal-state spyware law enforcement task force to discuss issues and trends in spyware law enforcement. The task force consists of representatives from agencies such as

⁸*In the Matter of Zango, Inc. f/k/a 180 Solutions, Inc.*, FTC Dkt. No. C-4186 (Mar. 7, 2007), available at <http://www.ftc.gov/os/caselist/0523130/index.shtm>.

⁹*In the Matter of DirectRevenue LLC*, FTC Dkt. No. C-4194 (June 26, 2007), available at <http://www.ftc.gov/os/caselist/0523131/index.shtm>.

¹⁰*FTC v. Digital Enterprises, Inc. d/b/a Movieland.com*, CV06-4923 (C.D. Cal. Sept. 5, 2007), available at <http://www.ftc.gov/os/caselist/0623008/index.shtm>.

¹¹*FTC v. MaxTheater, Inc.*, No. 05-CV-0069 (E.D. Wa. Dec. 6, 2005), available at <http://www.ftc.gov/os/caselist/0423213/0423213.shtm>.

¹²*FTC v. Trustsoft, Inc.*, No. H-05-1905 (S.D. Tex. Nov. 30, 2005), available at <http://www.ftc.gov/os/caselist/0523059/0523059.shtm>.

¹³See, e.g., Department of Justice, Computer Crime & Intellectual Property Section, Computer Crime News Releases, available at <http://www.usdoj.gov/criminal/cybercrime/ccnews.html>.

¹⁴*FTC v. ERG Ventures, LLC*, 3:06-CV-00578-LRH-VPC (D. Nev. Oct. 3, 2007), available at <http://www.ftc.gov/os/caselist/0623192/index.shtm>. Pursuant to the stipulated order entered by the court in the FTC action, the defendants must disgorge \$330,000. A permanent injunction also bars the defendants from downloading software onto consumers' computers without disclosing its function and obtaining consumers' consent prior to installation, bars them from downloading software that interferes with consumers' computer use, and bars false or misleading claims.

¹⁵See FTC News Release, *Court Shuts Down Media Motor Spyware Operation* (Nov. 13, 2006), available at <http://www.ftc.gov/opa/2006/11/mediamotor.shtm>.

the Department of Justice and state attorneys general. Federal criminal and state law enforcement actions are a critical complement to the FTC's law enforcement actions.

III. Education

In addition to engaging in law enforcement, the FTC has made consumer education a priority. In September 2005, the Commission and a partnership of other Federal agencies and the technology industry launched a multimedia, interactive consumer education initiative, OnGuard Online, along with a Spanish-language version, AlertaenLinea. The *OnGuardOnline.gov* site now attracts over 350,000 unique visits each month, and many organizations have adapted the OnGuard Online materials for their own security training. The comprehensive website has general information on online safety, as well as sections with specific information on a range of topics, including spyware. The spyware module includes up-to-date information, as well as interactive features like quizzes and videos. As part of the OnGuard Online initiative, the FTC also has distributed a million copies of the brochure and two million copies of the bookmark, "Stop Think Click: 7 Practices for Safer Computing," with information on spyware and other computer safety topics. The FTC also has issued a Consumer Alert on spyware, as well as Alerts addressing other online security issues such as viruses and peer-to-peer file sharing.¹⁶

IV. Legislative Steps to Address Spyware

Although the FTC has successfully challenged conduct related to spyware dissemination under Section 5, legislation authorizing the Commission to seek civil penalties in spyware cases could add a potent remedy to those otherwise available to the Commission. Currently, under Section 13(b) of the FTC Act, the Commission has the authority to file actions in Federal district court and to obtain injunctive relief and equitable monetary relief in the form of consumer redress or disgorgement. It has been the agency's experience in spyware cases, however, that restitution or disgorgement may not be appropriate or sufficient remedies because consumers often have not purchased a product or service from the defendants, the harm to consumers may be difficult to quantify, or the defendants' profits may be slim or difficult to calculate with certainty. In such cases, a civil penalty may be the most appropriate remedy and serve as a strong deterrent. Accordingly, the Commission is pleased that S. 1625 provides the Commission this valuable law enforcement tool.

Last June, FTC staff provided this Committee with technical comments to S. 1625. Of the various suggestions respectfully made by staff, one important aspect of the bill relating to both injunctive relief and civil penalties stands out. Under general consumer protection principles and traditional Section 5 jurisprudence, the Commission need not show knowledge or intent in order to obtain injunctive relief: that is, for stopping the violative conduct itself. But, several sections of S. 1625 impose an overarching knowledge or intent threshold for enforcement that could create an additional—and often very challenging—evidentiary burden for the FTC in obtaining injunctions in civil cases. Moreover, Section 5(m)(1) of the FTC Act already requires the Commission to prove knowledge in any action where civil penalties are sought. Eliminating the knowledge or intent threshold from the bill would not change the Commission's elevated burden regarding civil penalties, while maintaining the ordinary burden for obtaining injunctive relief.¹⁷ The agency looks forward to working with the Committee regarding the knowledge and intent aspects of the legislation, as well as any of the other important considerations raised by staff's technical comments.

V. Conclusion

The FTC will continue its 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 the opportunity to discuss the Commission's law enforcement program.

¹⁶ See, e.g., *P2P File-Sharing: Evaluate the Risks* (Feb. 2008), available at <http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt128.shtm>; *Botnets and Hackers and Spam (Oh, My!)* (June 2007), available at <http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt132.shtm>; *Spyware* (July 2005), available at <http://www.ftc.gov/bcp/conline/pubs/alerts/spywarealrt.shtm>; *Detect, Protect, Disinfect: Consumers Online Face Wide Choices in Security Products* (Sept. 2004), available at <http://www.ftc.gov/bcp/conline/pubs/alerts/idsalrt.shtm>; see generally <http://www.ftc.gov/bcp/menus/consumer/tech/privacy.shtm>.

¹⁷ Indeed, removing the knowledge or intent requirements from S. 1625 would be consistent, for example, with the approach in the CAN-SPAM Act. See 15 U.S.C. § 7706(e) (granting the FTC authority to seek cease-and-desist orders and injunctive relief without alleging or proving knowledge). Spam raises similar enforcement issues to spyware regarding quantifying consumer injury and defendants' profits.

Senator NELSON. Senator Vitter?

Senator VITTER. Thank you, Mr. Chairman.

Thank you very much for your testimony. In October 2005, then Chairman Majoras had a discussion with Senator Allen about these issues and I believe Senator Allen asked if new notice and consent requirements would help combat spyware. The then Chair testified that she didn't think that it would do so because studies showed the more consumers are bombarded with disclosure and consent requirements the more they don't read them and sort of let them pass by and ignore them. What's your reaction to that question?

Ms. HARRINGTON. I think probably our view has not changed, but, more importantly, I think the nature of the spyware problem has shifted some, from the sort of pervasive pop-up and nuisance ads that adware brought us, to far more malicious and malevolent consequences from spyware.

I think that it's very unlikely that criminals using spyware to take over consumers' computers and cause them to do bad things would comply with notice requirements. These are criminals and their stock in trade is to sneak around.

Senator VITTER. OK. What do you think our general approach should be in terms of how technology specific we have to be or to what extent we can avoid that?

Ms. HARRINGTON. Well, we certainly know from what is really a very brief period of time during which the Internet has operated as a principal method of commerce that the technology shifts very quickly. To the extent that the Congress chooses to legislate in this area, I recommend staying away from specific technology and favoring broad principles like those that are found in Section 5 of the FTC Act, which as an enforcement tool has proven over the decades to be a marvelously flexible and resilient statute. The FTC Act was adopted in the earlier part of the 20th century and it has stood us very well. It is the statute that we have used to stop spyware purveyors in 11 enforcement actions. That kind of flexibility in a statute is very helpful when the technology changes virtually overnight.

Senator VITTER. OK, that's all I have right now, Mr. Chairman.

Senator NELSON. Ms. Harrington, you note that one of the Commission's spyware enforcement principles is a consumer should be able to uninstall or disable unwanted spyware. In the *Zango* and *DirectRevenue* consent orders, this principle was interpreted requiring those parties to provide a readily identifiable means to uninstall. How is that readily identifiable means identified? How is it defined?

Ms. HARRINGTON. The order sets the standard. The test is whether a reasonable consumer having the experience of having that software loaded onto his or her computer can readily see how it is that it can be uninstalled. It's really a reasonable consumer standard that's incorporated in those orders.

Senator NELSON. So it's not a case by case analysis?

Ms. HARRINGTON. Well, do you mean for purposes of complying with that order, Senator, or across the board?

Senator NELSON. Of defining it.

Ms. HARRINGTON. Well, we would always look case by case to see whether—but employing the reasonable consumer standard. That

is how the Commission proceeds also in using Section 5 as an enforcement tool and it is how the courts have interpreted Section 5 and ordered relief.

Senator NELSON. Do you need to include an operating system toolbar?

Ms. HARRINGTON. Do you need to?

Senator NELSON. Does the readily identifiable means need to include an operating system toolbar?

Ms. HARRINGTON. I'm going to turn to one of our lawyers who's right behind me who worked on that case.

Senator NELSON. Does the—

Ms. HARRINGTON. I don't want to give a wrong answer.

Senator NELSON. OK, come on up.

Ms. HARRINGTON. It doesn't necessarily require a toolbar, Senator, but we would generally think that the consumer would look to the add-remove function to find and remove the software. Or there could be a link that the consumer could use to get to the add-remove.

Senator NELSON. And if it's another kind of spyware, there would be another kind of toolbar to remove?

Ms. HARRINGTON. Any software that would be loaded onto the consumer's computer would need to be easily found and removed. I think generally we would expect that it would be very apparent when the add-remove function is chosen. But a link would work as well.

Senator NELSON. Do you think some clear rules or definitions might be helpful to consumers so that they would know where to look for this uninstall tool?

Ms. HARRINGTON. I think that generally, that the standard that requires that it be readily apparent and useable would be a better standard in a situation where the technology and format are changing frequently. So I would be concerned about tying by rule to a particular technique for removal. I think that the better approach would be to require that it be readily apparent and accessible to consumers, and we would assume that over time what that means would change; in very specific terms what it means would change with the technology.

Senator NELSON. What if the spyware is a keystroke logger and it's capturing all of the keystrokes that the computer user uses, such as it is trying to get passwords or personal information?

Ms. HARRINGTON. Well, that's criminal.

Senator NELSON. It is. But what about a toolbar to remove that? How would you go about that?

Ms. HARRINGTON. How would I go about that? I think that it would be unlikely, frankly, that someone installing a keystroke logger would willingly put a clear and apparent tool right before the consumer to alert him or her to the fact that the keystroke logger has been loaded on and to allow them to remove it. The whole purpose of that kind of software is to surreptitiously steal information from consumers.

Senator NELSON. So how does the consumer clean his computer of that spyware?

Ms. HARRINGTON. It may be that the consumer's security program that presumably includes a scan function that can be regu-

larly run, will identify that program. Typically, when you run those kinds of scans you get a box with a report that tells you what you have and it's really easy to remove.

If the software can't be detected by those kinds of programs, and the really bad stuff that we're talking about oftentimes flies under that radar, the consumer may not be able to discern its presence on his or her computer until something really bad happens, and then the consumer has to backtrack to try to figure out how his or her information fell into the hands of bad guys. It may be very tough for consumers to know that they have that kind of software on their computer.

Senator NELSON. What percentage of the spyware do you think currently originates outside of the United States?

Ms. HARRINGTON. We don't have a way of measuring that, but we certainly know that there are problems with malevolent software that shows up through spyware, through e-mail on people's computers. We know that there are big problems with that kind of material originating outside of the United States. But we don't have a way of measuring it, just as we don't have a way of measuring the totality of spyware that's loaded onto consumers' computers, whether it comes from within or outside of the United States.

Senator NELSON. Do we need to give the FTC new tools to go after these foreign bad actors?

Ms. HARRINGTON. Well, we're very grateful to the Congress for having given us some new tools a couple of years ago in the U.S. SAFE WEB Act. We have enhanced authority now to share information with foreign counterparts and obtain information from them, and we are using it in nonpublic investigations all the time, and we're most appreciative of the Congress for giving us those authorities.

Senator NELSON. So we have enough? We don't need more?

Ms. HARRINGTON. We're in good shape now, thank you.

Senator NELSON. How well do commercial anti-spyware applications work?

Ms. HARRINGTON. Well, some work well and some don't work well. Some anti-spyware applications are actually hawked by crooks to put more spyware on your computer instead of taking it off. So there's quite a spectrum of performance. But the reputable software companies that are selling anti-virus and security software sell reasonably good products, and if you visit our OnGuardOnline website, we recommend that everyone make sure to have good security programs on their computer and run them regularly.

Senator NELSON. Well, the government and the commercial anti-spyware providers seem to have been talking for quite a while now and still the message isn't getting out to a lot of consumers. How can we do it better?

Ms. HARRINGTON. Well, first of all, we would urge everyone, every government and commercial entity that cares about this to have a link to OnGuardOnline right on their website. It is a very consumer-friendly site with really easy-to-understand and use directions about how to protect your computer from a host of bad

things and how to prevent oneself from experiencing bad experiences in the online environment.

So help us get the message out. I think that to the extent that the manufacturers of anti-spyware software and other security products can continue to make these products very user friendly, anything that we can do to encourage movement in that direction is a good thing. These products have become far more user friendly. I know, I can actually use them reasonably well myself now and I used to find them to be quite difficult.

Senator NELSON. Yesterday's *New York Times* carried a story about the Attorney General of New York going after child pornography and it seemed like an inventive way that he was doing it, by going and holding the people who convey the information accountable. First of all, would you comment on what it is, explain it, and then tell us what you think about it?

Ms. HARRINGTON. Well, I've read the same press accounts that you have. That's what I know about this. But my understanding is that the agreement that the attorney general of New York entered into is with three large ISPs, and the ISPs have agreed to block their users from accessing sites that have been identified as containing child pornography material.

This is an agreement or a settlement. I don't know what the underlying legal theory is. I noted in some of the press accounts that I read this morning that some are raising First Amendment concerns. Beyond that, I really don't know more about that agreement.

Stepping back, there are certainly times when companies that operate portals or control the means of access have been able to step up and use that influence and leverage to shut off or discourage bad activity. That's not a new approach. I really don't know about this particular settlement and how effective it will be at eliminating the problem that they're seeking to address.

Senator NELSON. Senator Vitter?

Senator VITTER. I'm fine. Thank you, Mr. Chairman.

Senator NELSON. Well, Ms. Harrington, thank you very much for your testimony.

Ms. HARRINGTON. Thank you, Senator.

Senator NELSON. We would ask the second panel to please come up.

We are very pleased to have Mr. Arthur Butler, who is with the Americans for Fair Electronic Commerce Transactions; Mr. Jerry Cerasale, who is Senior Vice President, Government Affairs with Direct Marketing Association; Mr. Marc Rotenberg, Executive Director, the Electronic Privacy Information Center; Dr. Benjamin Edelman, who is at the Harvard Business School; Mr. Vincent "WAE-fer"——

Mr. WEAFFER. "WEE-fer."

Senator NELSON. "WEE-fer," who is Vice President, in Security Response with the Symantec Corporation, and on behalf also of the Business Software Alliance.

We'll start in the order that you are listed on the agenda. Mr. Butler. And what I want you to do, I don't want you to sit here and read a statement to us. We're going to take your printed statements. That's going to be a part of the record. So what we want you to do is talk to us.

So, Mr. Butler.

**STATEMENT OF ARTHUR A. BUTLER, ATTORNEY, ATER WYNNE
LLP, ON BEHALF OF AMERICANS FOR FAIR ELECTRONIC
COMMERCE TRANSACTIONS (AFFECT)**

Mr. BUTLER. Good afternoon. My name is Art Butler. I'm an attorney with the Ater Wynne law firm in Seattle, Washington, and I'm here today on behalf of AFFECT, which is a diverse group of nonprofits and commercial entities, including consumer groups, who are firmly committed to promoting the growth of fair and competitive transactions in software and other digital products.

I first wanted to commend Senator Pryor and the other cosponsors of the Counter Spy Act for introducing what we think is a very important piece of legislation and for holding this hearing, because you, like the members of AFFECT, are very worried about the privacy and security issues that are presented by spyware.

As our long statement indicates, we firmly support S. 1625 because we believe that spyware is an insidious problem that desperately needs to be addressed. The sad fact is that every computer in the United States is under attack from numerous sources that are trying to surreptitiously install or prevent the removal of spyware programs that will allow the spies to intercept or gain partial control of the user's interaction with his or her computer without obtaining the user's informed consent.

Often the spyware that is introduced contains what are called back doors, which essentially are ways in which a computer spy can get around normal authentication and remotely gain control over the computer and avoid detection. Once someone gains control of your computer, they can install all kinds of different devices to compromise the security of that computer. In fact, it is generally agreed that spyware represents a significant threat to the security of any user's computer system and data.

While we support the bill, we do have a major concern with the exceptions section of the bill. That is due to, one, the fact that really we don't see that any of the exceptions that are listed there are really needed or justified. But we're particularly concerned about the exception in subsection 6(a)(10) which would permit a provider to monitor or interact with a computer in order to prevent or detect the unauthorized use of software, fraudulent or other illegal activities.

We think this language is overly broad and it would in effect permit or protect activities which could be harmful to computer users in direct opposition to the objective of the bill. It would in effect allow a software vendor to freely monitor everything that's on a user's computer, essentially setting them up as an ad hoc police force to conduct warrantless searches and seizures. We don't think that private entities should be allowed to engage in law enforcement activities.

The most troubling fact to us is the fact that that language would permit a software vendor to unilaterally remotely disable the software on a computer or to disable a network connection or service. Often the question about whether use is unlawful or fraudulent or illegal is subject to legitimate dispute, and it really merits some

judicial consideration before you allow a software vendor to unilaterally employ such a drastic remedy as remote disablement.

This is a major concern to our members and we have in our long statement given examples of cases where you have seen software purveyors unilaterally decide that they didn't get an adequate license payment and then just go in and shut down someone's computer, causing some very significant negative consequences for the computer user.

But it's also important to realize that a lot of these disputes never make it to the courthouse steps because the balance of harm that's caused by someone unilaterally shutting down your computer is so far against the computer user that the mere threat that that can be used will cause the user to essentially cave in to the demands of a vendor.

We are particularly concerned about what happens when someone remotely accesses a computer and attempts to disable it because that act alone can cause damage to other files owned by the computer user and the simple fact is that the existence of that code that allows remote access and disablement can present a vulnerability that will allow security breaches by hackers, by saboteurs, by industrial and foreign government spies, and by terrorists.

This is a major issue for our group, for both the smaller users and the large users. We have a suggestion for an amendment to subsection 6(a)(10) that would essentially limit that to the detection or prevention of fraudulent or other illegal activities as prohibited by the Act, which we think is the appropriate limitation there.

Thank you. I'd be glad to respond to any questions.

[The prepared statement of Mr. Butler follows:]

PREPARED STATEMENT OF ARTHUR A. BUTLER, ATTORNEY, ATER WYNNE LLP, ON BEHALF OF AMERICANS FOR FAIR ELECTRONIC COMMERCE TRANSACTIONS (AFFECT)

Good afternoon. My name is Art Butler. I am an attorney with Ater Wynne LLP in Seattle, Washington. I am very pleased to appear before you today on behalf of AFFECT (Americans for Fair Electronic Commerce Transactions) at this important hearing on the impact and policy implications of spyware on consumers and businesses. AFFECT is a national coalition of consumer representatives, retail and manufacturing businesses, insurance institutions, financial institutions, technology professionals, librarians, and public interest organizations committed to promoting the growth of fair and competitive commerce in software and other digital products.

We commend you, Chairman Pryor, and all the sponsors of the Counter Spy Act (S. 1625), for introducing this important bill because, like you, our members are very worried about the privacy and security risks associated with spyware. AFFECT strongly supports S. 1625. However, we are very concerned with the exception provision and believe it is overly broad. In our view, it could in fact be construed to protect wrongful acts that can result in great harm to computer users. We believe this section is in direct opposition to the laudable purpose of the bill and hope very much that you will consider the amendment which we propose today.

AFFECT's Concerns with Spyware

AFFECT has been active in representing the interests of software consumers in the debates about the appropriate language to be included in anti-spyware legislation in several states and has advocated strenuously that these legislatures not adopt exception language so broad that it swamps the prohibitions that are designed to protect computer users. Since AFFECT began actively educating legislators in the states of the potential for damage, creation of security vulnerabilities, and for invasion of privacy and unauthorized search and seizure in relation to consumers' computers due to the exception language in question—the language has failed to pass in even one state legislature.

The sad fact is that every computer in the United States is under attack from numerous sources trying to surreptitiously install or prevent removal of spyware

that will allow the spy to intercept or take partial control over the user's interaction with the computer, without the user's informed consent.

While the term "spyware" suggests software that secretly monitors the user's behavior, the functions of spyware extend well beyond simple monitoring. Spyware can collect various types of personal information, interfere with the user's control of the computer, change computer settings, result in slow connection speeds, loss of Internet or other programs, disable software firewalls and anti-virus software, and/or reduce browser security settings, thus opening the system to further infections. It can enable identity theft and fraud.

Often spyware will contain a "backdoor," which is a method of bypassing normal authentication, securing remote access to a computer and obtaining access to plaintext, while attempting to remain undetected. Someone who has gained access to your computer can install many types of devices to compromise security, including operating system modifications, software worms, key loggers, and covert listening devices. Some backdoors, such as the Sony/BMG rootkit¹ distributed silently on millions of music CDs through late 2005, are intended as digital rights management (DRM) measures and, in that case, as data gathering agents, since both surreptitious programs they installed routinely contacted central servers. The copy prevention software Sony/BMG included on its CDs was automatically installed on Windows desktop computers when customers tried to play the CDs. The software interferes with the normal way in which the Microsoft Windows operating system plays CDs, opening security holes that allow viruses to break in, and causing other problems.²

It is generally agreed that spyware represents a significant threat to the security of any computer owner's data. Even for large enterprises spyware represents a serious threat to the integrity of intellectual property, confidential data, and personally identifiable information of employees and customers. Accordingly, AFFECT supports legislative efforts, like S. 1625, that are designed to curb the use of harmful spyware.³

AFFECT's Concerns with the Exception Provision of S. 1625

AFFECT has concerns with the exception section of S. 1625, section 6, which is overly broad and could be construed to protect wrongful acts that can result in great harm to computer users in direct opposition to the purpose of the bill.

We are particularly concerned about Subsection 6(a)(10), which would permit a provider to monitor or interact with an individual's computer, or Internet or other network connection or service for the "detection or prevention of the unauthorized use of software fraudulent or other illegal activities." The reference to "unauthorized" is too vague and raises a number of questions. "Authorized" by whom? What is the process for authenticating the identity of the person using the software? And what are the standards for determining whether that person has the authority to perform a certain operation, and who decides?

This language would allow a software vendor to surreptitiously download code onto a user's computer and freely violate the user's privacy by monitoring everything on his or her computer, as long as it did so under the guise of looking for unauthorized use, fraudulent, or illegal activities. It would allow the provider to set itself up as an ad hoc police force to conduct warrantless searches and to act as judge and jury to conduct unilateral seizures. Private entities *do not* and *should not* have the right to conduct law enforcement activities.

More troubling is the fact that the language of Subsection 6(a)(10) would effectively allow a software provider to unilaterally decide to remotely shut down the user's computer or Internet or other network connection or service. But whether the use of a particular software is "unauthorized," "fraudulent," or "illegal" is often subject to legitimate dispute and merits some judicial consideration before a provider is allowed to unilaterally employ a drastic remedy like remote disablement.

Permitting unilateral remote disablement is simply bad public policy. Unilateral remote disablement can cause great harm to any computer owner who depends on

¹A "rootkit" is a program designed to take fundamental control of a computer system, without authorization by the system's owners and legitimate managers. Typically, rootkits act to obscure their presence on the system through subversion or evasion of standard operating system security mechanisms. Often, they are also Trojans as well, fooling users into believing they are safe to run on their systems.

²As a result, a number of parties filed lawsuits against Sony/BMG; the company eventually recalled all the affected CDs.

³S. 1625 (Pryor), introduced in June 2007, would protect against the unauthorized installation of software that is used to take control of a computer in order to cause damage, collect personal information without consent, or otherwise enable identity theft.

access to and use of that computer, connection or service. For example, the shut-down of an owner's system can cause great harm to:

- a teacher using a computer to prepare for classroom lectures;
- an insurer depending on a computer system to pay claims;
- a manufacturer trying to deliver its products to meet contractual commitments;
or
- the public's access to online library materials.

That harm can be significantly larger than the harm to the software vendor (not getting a license fee).

Even large enterprises are concerned about the threat of remote disablement. There have been a number of reported cases where software developers unilaterally determined that licensees didn't make appropriate payments and simply shut down the computer programs.⁴ The most widely reported was a case where a small software developer, Logisticon, Inc., installed malware within warehouse-management software delivered to cosmetic company, Revlon Inc. When the parties got into a dispute over whether the software had bugs and didn't perform as promised, Revlon withheld payment. Logisticon then tapped into Revlon's computers and disabled the program, which paralyzed Revlon's shipping operations for 3 days. Losses to Revlon were about \$20 million. Revlon sued, charging extortion. Logisticon claimed this was simply "electronic repossession." The case was settled out of court.

Clearly many disputes never make it to the courthouse steps because the balance of harm to be done via exercise of remote disablement is so overwhelmingly against the computer user that the mere threat of its use puts the user in an unfair position, and it must cave to the demands of the software vendor. The ability to unilaterally disable a user's computer or critical software running on it provides the software, network, or service provider undue leverage in a dispute even if the remedy is not exercised. Faced with a crippling and possibly even fatal disruption of its business, a user could be intimidated into relinquishing its rights and setting up precedents for its further disadvantage. This is because the risk to the provider that it will be held to have acted improperly is indefinite and its potential liability severely limited. Even if a provider wrongly exercises the remote disablement, it is unlikely the injured user will be able to recover money damages for the harm resulting from this action, including losses to the user's business attributable to the wrongful act, because providers routinely disclaim consequential damages in their licensee agreements; in fact, they routinely limit recoverable damages to the amount of the license fee.

⁴Other cases include the following: In 1998 in *Franks & Sons, Inc. v. Information Solutions, Inc.*, the software developer installed a "drop-dead" code in the program. When the customer failed to pay as promised, the developer activated the drop-dead code, which prevented the customer from accessing the software as well as any stored information. The customer didn't know about the drop-dead code, and the court found that it would be unconscionable to allow the software developer to hold the licensee ransom as it did.

In 1991, in *American Computer Trust Leasing v. Jack Farrell Implement Co.*, 763 F. Supp. 1473 (D. Minn. 1991), the software developer, in a dispute over payment for the software, remotely deactivated the software. The contract provided that the developer, who owned the software, could remotely access the licensee's computer in order to service the software and that, if the licensee defaulted, the agreement was canceled. When the licensee didn't pay, the developer told the licensee that it was going to deactivate the program, which it promptly did. The licensee sued for damages, but the court ruled in favor of the developer on the grounds that the deactivation was "merely an exercise of [the developer's] rights under the software license agreement . . ."

There have been many other cases involving software developers either putting drop-dead code in their products or remotely disabling code when they thought the other party was in breach. For example, a Dallas medical device software developer was sued in 1989 for using a phone line to deactivate software that compiled patients' lab results. The case was settled. In 1990, during a dispute about the performance of a piece of code, the developer simply logged in and removed the code, until the licensee released the developer from any liability. The licensee claimed that the general release was signed under duress, since he was being held economic hostage. *Art Stone Theatrical Corp. v. Technical Programming & Support Systems, Inc.*, 549 N.Y.S. 2d 789 (App. Div. 1990).

In 1991, in *Clayton X-Ray Co. v. Professional Systems Corp.*, 812 S.W.2d 565 (Mo. Ct. App. 1991), a company involved in a payment dispute logged into the licensee's computer and disabled the software. When the licensee tried to log on to see its files, all it saw was a copy of the unpaid bill. A jury awarded the licensee damages.

In *Werner, Zaroff, Slotnick, Stern & Askenazy v. Lewis*, 588 N.Y.S. 2d 960 (Civ. Ct. 1992), a law firm contracted with a company to develop billing and insurance software. When the software reached a certain number bills, and when the developer decided it had not been paid sufficiently, it shut down the software disabling access to the law firm's files. The law firm sued successfully.

Moreover, in reaching into an individual's computer remotely to disable software residing on that computer, the software provider may not only violate privacy rights, but also damage the computer owner's other files. And the monitoring and remote disablement of software on an owner's computer by an outsider may compromise private information of employees, confidential and proprietary information of the owner, and, in some cases, national security information. As a result, it is possible that they could put an owner into breach of obligations it has under other laws (*e.g.*, Health Insurance Portability and Accountability Act).

The simple fact is that the code used to remotely enter a computer and disable the software or the network connection makes the computer vulnerable to security breaches by hackers, saboteurs, industrial and foreign governmental spies, and terrorists. The consequences of a successful intentional or even accidental misuse of a computer system range from loss of confidentiality to loss of system integrity, which may lead to more serious concerns, like data theft or loss, or, in the case of a business, significant financial losses or worse. When there is an opportunity to negotiate, many enterprises, including governmental entities, will insist that their software license agreements contain a warranty prohibiting any "self-help code" or other software routing designed to disable a computer program automatically or that is under the positive control of a person other than the licensee of the software. Unfortunately, with mass market licenses individual consumers and businesses are not able to negotiate for a "no self-help code" warranty.

Proposed Amendment

S. 1625 is a commendable piece of legislation that addresses a real problem faced by computer users throughout this country. AFFECT supports it, but strongly recommends that the exception provision of S. 1625 should *only* limit liability for interaction with a network, service, or computer that is undertaken to detect or prevent fraudulent or other illegal *activities as prohibited by the act itself*. Therefore, AFFECT proposes that Section 6(a)(10) of the bill be amended as follows:

"(10) detection or prevention of ~~the unauthorized use of software~~ fraudulent or other illegal activities *as prohibited by this Act*."

Conclusion

On behalf of AFFECT, thank you very much for the opportunity to appear before you today and for your consideration of our concerns. I would be happy to answer any questions you might have.

Senator NELSON. Mr. Cerasale?

STATEMENT OF JERRY CERASALE, SENIOR VICE PRESIDENT, GOVERNMENT AFFAIRS, DIRECT MARKETING ASSOCIATION, INC.

Mr. CERASALE. Senator Nelson, Members of the Committee: Thank you for the opportunity to appear here today. I'm Jerry Cerasale, Senior Vice President for Government Affairs for the Direct Marketing Association, an association of 3,600 marketers who present offers and services to consumers directly.

It is important in that kind of a business model that we have trust, that the consumer trust the marketer, but the consumer also has to trust the channel of marketing, and that's what we're here talking about today. In the past 3 years we have moved quite a ways in trying to prevent spyware, and I think we have to praise quite a few groups. One is Congress for constantly looking at this and putting pressure on us.

The second are the software vendors, one of whom is sitting here on the table with me, for producing excellent products to go after and being able to remove objectionable software.

Third, organizations, TRUSTe and even DMA, for setting up guidelines and establishing education. DMA has worked with, partnered with, the Federal Trade Commission and OnGuard Online.

Finally but not least, law enforcement, looking at the Federal Trade Commission, the Department of Justice, and the State Attorneys General, pursuing bad actors.

DMA supports removal of objectionable software and the means to do that. Our guidelines that we produce that all our members have to follow—and it's attached to my larger testimony—bans or prohibits putting on software that takes over someone's computer. It requires for installing other software that there be notes, that there be an easy means to uninstall or disable the program, that there be contact information concerning the organization that put the software on the computer so that the consumer can contact them, and that there be an easy, identifiable link to the privacy policy of that organization.

So we have taken these steps and will continue to look at it more, and we had to write these guidelines in looking at it being not technologically, not focused on one technology, but to try and be broader so that as we get changes tomorrow and the next day, that we do not have to go back and rewrite our guidelines.

We have a few specific comments concerning S. 1625. As we look at Section 4(b)(2) of the bill, we think also that this can be read very broadly and can in fact be used to cover legitimate advertising practices, those same practices that have helped create Cyber Monday to be a larger shopping day than Black Friday or support the great amount of free content on the Internet.

We think, our suggestion is, in the previous Congress Section 4(b)(2) had an additional provision in it dealing with bad acts, and we think that that is a suggestion we have for Section 4(b)(2).

As we look on, and I have to comment on Section 6(a)(10), one of the things to be careful about when looking at legislation or regulation in anti-fraud arenas is that we have, many of our members have anti-fraud provisions and those are out there to protect users from identity theft, and they have been fairly successful and successful in stopping credit card fraud and so forth. So as you look at things looking at the exceptions in 6(a)(10) is to make sure that we don't have unintended consequences there.

Finally, 6(a)(8) and (9), giving limited liability. Our concern here is that it will remove accountability for software vendors. We think that this is very important, to have this accountability. Objectionable software is a subjective term and you can disagree on it. Many DMA members have written to and contacted software vendors whose software has removed their particular software on someone's computer and they have been able to work it out, very, very reputable organizations. Sometimes there has not been a resolution, and where do you go if there's not a resolution on this subjective term?

Finally, there are some software vendors who don't answer phone calls, who don't respond to letters, and who don't respond to e-mails. If you have this kind of argument on a subjective issue, where do you go? So we're very concerned that you, Congress not eliminate accountability.

Thank you very much.

[The prepared statement of Mr. Cerasale follows:]

PREPARED STATEMENT OF JERRY CERASALE, SENIOR VICE PRESIDENT,
GOVERNMENT AFFAIRS, DIRECT MARKETING ASSOCIATION, INC.

I. Introduction and Summary

Good morning, Mr. Chairman and Members of the Committee. I am Jerry Cerasale, Senior Vice President for Government Affairs of the Direct Marketing Association, and I thank you for the opportunity to appear before the Committee as it examines S. 1625 and the spyware issue in general.

The Direct Marketing Association, Inc. ("DMA") (www.the-dma.org) is the leading global trade association of businesses and nonprofit organizations using and supporting multichannel direct marketing tools and techniques. DMA advocates industry standards for responsible marketing, promotes relevance as the key to reaching consumers with desirable offers, and provides cutting-edge research, education, and networking opportunities to improve results throughout the end-to-end direct marketing process. Founded in 1917, DMA today represents more than 3,600 companies from dozens of vertical industries in the U.S. and 50 other nations, including a majority of the Fortune 100 companies, as well as nonprofit organizations. Included are catalogers, financial services, book and magazine publishers, retail stores, industrial manufacturers, Internet-based businesses, and a host of other segments, as well as the service industries that support them.

DMA and our members appreciate the Committee's outreach to the business community on this important issue. I note at the outset that this is a complicated issue. In part due to congressional attention, over the past several years there have been significant developments that have fundamentally improved the consumer experience as it relates to spyware. Where once, just three short years ago, invasive pop-up ads, drive-by downloads, and software that hijacked computers were on the rise, consumers in 2008 experience fewer such unwanted practices. Industry guidelines for legitimate software downloads, strong self-regulation, major technological improvements, and Federal Trade Commission ("FTC") and state Attorney General enforcement have all contributed to the current, significantly improved environment where the prevalence of spyware has been vastly reduced. While DMA supports the Committee's interest in combating spyware, given that the marketplace has evolved considerably since previous Congresses considered this issue, we believe that a statutory approach that would cover a broad range of software downloads and online marketing might not achieve the desired purpose of limiting spyware, but might have the unintended effect of interfering with important e-commerce and marketing functionalities.

Internet growth over the past 10 years has been nothing short of remarkable, and this growth is fueled by the seamlessness of interactions of content, software, advertising, and other services. The dramatic rise of the Internet is evident in the dollar amounts consumers spend purchasing products through Internet sales. Last year, on Cyber Monday, the busiest Internet shopping day of the year, shoppers spent more than \$733 million online.¹ This represents an increase of 21 percent from the same day the previous year and is more than the amount shoppers spent on Black Friday.²

Additional statistics demonstrate the staggering growth in e-commerce. The U.S. Census Bureau, which releases quarterly retail e-commerce statistics, recently reported that estimated retail e-commerce sales for the 1st quarter of 2008 were \$33.8 billion, an increase of 13.6 percent from the 1st quarter of 2007. The Census Bureau also noted that 1st quarter e-commerce sales accounted for 3.4 percent of total sales.³

As these and similar figures suggest, the Internet revolution has had a tremendous impact on economic growth. The Internet has become a preferred mechanism of commerce for many consumers, and a key part of multi-channel sales efforts for businesses. This phenomenon has changed the way products and services reach the market, and enables consumers to shop in an environment that knows no restrictions on time or place.

¹ Cyber Monday is the first Monday following Thanksgiving. In 2007, Cyber Monday fell on November 26. The Friday after Thanksgiving Day is known as Black Friday and is traditionally the largest brick and mortar shopping day of the year.

² See <http://www.comscore.com/press/release.asp?press=1921>.

³ U.S. Census Bureau, *Quarterly Retail E-commerce Sales, 1st Quarter 2008*, May 15, 2008. See <http://www.census.gov/mrts/www/data/pdf/08Q1.pdf>.

II. Strong Guidelines, Technology, and Enforcement Have Reduced the Need for Legislation

The combination of strong industry guidelines, anti-spyware technologies, and enforcement of existing laws over the past 3 years has limited pernicious software downloads, reducing spyware's threat to the positive consumer experience online. Together, we are winning the battle against such malicious practices. That said, this battle will be ongoing. Today's solutions and remedies may be obsolete tomorrow. As technology continues to evolve rapidly, so too will the challenges posed by spyware and related bad practices.

A. Industry Guidelines

DMA has long been a leader in establishing comprehensive self-regulatory guidelines for its members on important issues related to privacy and e-commerce, among many others. DMA and its member companies have a major stake in the success of electronic commerce and Internet marketing and advertising, and are among those benefiting from its growth. Our members understand that their success on the Internet is dependent on consumers' confidence in the online medium, and they support efforts that enrich a user's experience while fostering consumer trust in online channels. Understanding the importance of standards and best practices in building consumer confidence, DMA, working with its members, in 2006 developed and adopted standards for software downloads as part of our *Guidelines for Ethical Business Practice* ("Guidelines"), to specifically discourage illegitimate software download practices that threaten to undermine electronic commerce and Internet advertising.⁴ In our experience, industry guidelines are the most effective way to address concerns that arise in the continuously changing technological landscape. Such guidelines are flexible and adaptable in a timely manner so as to cover bad practices and not unintentionally or unnecessarily cover legitimate actors. These software guidelines and an analysis of their requirements are attached.

B. Current Law Enforcement Efforts

Technology, self-regulation, and enforcement of existing laws are adequately addressing the problems caused by spyware. In the past couple of years, law enforcement officials have been using existing enforcement tools to pursue sources of spyware. The FTC has aggressively pursued adware companies engaging in improper business practices. Since 2004, the Commission has brought more than 10 such cases under its deceptive and unfair practices authority.⁵ In addition, the Department of Justice ("DOJ") is actively combating spyware under the Computer Fraud and Abuse Act and the Wiretap Act, also with more than 10 cases to date.⁶ The states have been an important part of the enforcement efforts in this area as well, with state attorneys general using their fraud and consumer protection laws to target distributors of spyware.⁷ Strong enforcement of existing laws, combined with industry self-policing and innovative technologies, thus, have drastically slowed the spread of spyware and its effects. As these efforts indicate, continued dedication of resources to enforcement has proven an effective response to spyware.

C. Marketplace Technology Has Adapted to Combat Spyware

The technological tools available to consumers to prevent spyware also have seen significant improvement in their effectiveness. These tools are highly sophisticated, user friendly, and widely available, and in many instances are available at no cost to the consumer. For instance, today's anti-spyware software is proactive in detecting malware before it can penetrate a consumer's personal computer, thereby eliminating frustrations of spyware by preventing it from ever being downloaded. Consumers also have access to new web browsers with stronger security features and better warning features. In addition, as spyware became a problem, industry re-

⁴Use of Software or Other Similar Technology Installed on a Computer or Similar Device, *DMA Guidelines for Ethical Business Practice*, at 21 (attached) (available at <http://www.the-dma.org/guidelines/EthicsGuidelines.pdf>).

⁵See, e.g., *In the Matter of DirectRevenue LLC*, FTC File No. 052-3131 (filed Feb. 16, 2007); *In the Matter of Sony BMG Music Entertainment*, FTC File No. 062-3019 (filed Jan. 30, 2007); *FTC v. ERG Ventures, LLC*, FTC File No. 062-3192 (filed Nov. 29, 2006); *In the Matter of Zango, Inc. f/k/a 180solutions, Inc.*, FTC File No. 052-3130 (filed Nov. 3, 2006).

⁶CFRA, 18 U.S.C. § 1030; Wiretap Act, 18 U.S.C. § 2511. See, e.g., *U.S. v. Jerome T. Heckenkamp*, <http://www.usdoj.gov/criminal/cybercrime/heckenkampSent.htm>; *U.S. v. Christopher Maxwell*, <http://www.usdoj.gov/criminal/cybercrime/maxwellPlea.htm>.

⁷For example, New York attorneys general over the past few years, as well as other attorneys general, have been actively pursuing cases against companies for deceptive practices in connection with spyware and adware. See New York Attorney General settlement with online advertisers, http://www.oag.state.ny.us/press/2007/jan/jan29b_07.html; settlement with DirectRevenue, http://www.oag.state.ny.us/press/2006/apr/apr04ab_06.html.

sponded by installing anti-spyware software onto personal computers before shipping them to customers. This service provides personal computers with an early vaccination against spyware.

III. Specific Concerns about S. 1625

I would like to take this opportunity to discuss specific comments regarding S. 1625, which is pending before the Committee. We believe that the significant developments described warrant reevaluation of certain provisions of this legislation by the Committee, which we hope that the sponsors of this bill and the members of the Committee will consider.

DMA is concerned that Section 4(b)(2) of the bill could create compliance uncertainty, which could, in turn, limit current and future critical e-commerce functions designed to make the Internet browsing experience seamless. For this reason, DMA believes that Section 4(b)(2) should be tailored to specifically target “bad practices,” rather than create the regulation of many legitimate information practices resulting from software. The current language in Section 4(b)(2) could be interpreted to extend well beyond regulating “surreptitious surveillance” practices. We recommend that any restriction on data collected and correlated with a user’s online history be narrowed, as this bill did the last time it was considered and approved by this Committee by adding the language contained in the previous bill. Our suggestion would apply only if the computer software was installed in a manner designed to conceal from a computer user the fact that the software was being installed and would perform an information collection function. This type of approach would make clear that the bill targets deceptive acts—which should be the objective of any such legislation—and does not restrain legitimate practices.

DMA also is concerned about Sections 6(a)(8) and (9), the provisions that would bestow limited liability on a business that removes “objectionable content” or software used in violation of the Act. While on its face, the authority to remove “objectionable content” may appear reasonable, the term “objectionable” is not defined and, as a consequence, section 6(a)(8) would allow any anti-spyware entity to act unilaterally, and without review, to block any material that it defines as “objectionable.” Under this authority, for example, an anti-spyware tool would be free to identify and remove anti-fraud software from a computer, with no liability for doing so, or for fraudulent activities that may then be perpetrated, or it could use the unfettered discretion provided for in this subsection to block a competitor’s access even if that competitor has the specific consent of the user. Moreover, it could do so without any notice whatsoever to the user. We are, therefore, concerned that this provision would grant full immunity to a business that oversteps its power to remove legitimate content and causes harm to another business or the user. This type of broad immunity would have negative consequences for consumers by undermining their personalized Internet experience. For instance, what may be “objectionable content” to an anti-spyware entity may be a consumer’s valued tool bar or personalized cookie.

For similar reasons, DMA has concerns about Section 6(a)(9), which would permit a business to remove software used in violation of sections 3, 4, or 5 the Act. In previous versions of this bill, this type of immunity has been referred to as a “Good Samaritan” provision. We are concerned that providing limited liability to providers acting under “Good Samaritan” protection may also have unintended consequences for consumers and businesses. DMA supports a provider’s ability to remove or disable a program employed to perpetrate a bad act. However, we are concerned that a provision as broad as Section 6(a)(9) would allow a provider to remove legitimate software without consequence. The current framework, under which existing laws are used to hold anti-spyware companies liable for removal of legitimate software, has served as an important check on overreaching by such providers and should be preserved.

In addition, the policy goal underlying a “Good Samaritan” exemption is unclear. This type of protection would limit liability for violations for providers of anti-spyware software that remove spyware from a computer. The operative provisions of Sections 3, 4, and 5 impose liability for causing the installation of software on a machine, not removing software. Thus, it is unclear why a provision limiting liability for “removal” of software is even necessary. Given the fact that it would limit liability where none exists in the first instance, DMA suggests that this provision be deleted.

Finally, DMA recommends that the exemption provided in the definition of “software” (Section 12(14)) be modified to include “cookies and any other software that performs a similar or identical function or functions.” By limiting the exemption solely to cookies, the bill is essentially regulating technology rather than conduct. As a result, the bill would foreclose the inclusion of new and innovative technologies

that perform a similar or identical function as a cookie. This type of limitation would stifle innovation.

IV. Conclusion

In summary, the combination of advances in industry self-regulation, enforcement, and technology, coupled with concerns about interfering with legitimate uses of software for marketing purposes, necessitates that certain sections of S. 1625 be revisited. If regulation is necessary, and we believe that it is unclear that a need for legislation remains in light of recent technological innovations, it should be drafted in manner that does not undermine current efforts or upset consumers' expectations regarding the types of available, legitimate online marketing.

I thank you for your time and the opportunity to speak before your Committee. I look forward to your questions and to working with the Committee on this legislation.

ATTACHMENT 1

Analysis of DMA Guidelines

The Direct Marketing Association requires member organizations to adhere to its *Guideline on Use of Software or Other Similar Technology Installed on a Computer or Similar Device*, which encourages members to provide notice and choice regarding software that may be downloaded onto a consumer's personal computer or similar devices (attached). This Guideline clearly states that marketers should not install, have installed, or use, software or other similar technology on a computer or similar device that initiates deceptive practices or interferes with a user's expectation of the functionality of the computer and its programs. Such practices include software that takes control of a computer, modem hijacking, denial of service attacks, and endless loop pop-up advertisements. This Guideline also is clear that businesses should not deploy programs that deceptively modify or disable security or browser settings or prevent the user's efforts to disable or uninstall the software. DMA's Ethics Policy Committee evaluates compliance with its guidelines and regularly publishes summaries of outcomes of matters considered. Penalties can include removal from membership, referral to the Federal Trade Commission, and public disclosure of concern.

This Guideline also details responsible practices for marketers offering software or other similar technology that is installed on a computer used to further legitimate marketing purposes. Specifically, such programs must provide a user with clear and conspicuous notice and choice at the point of joining a service or before the software or other similar technology begins operating on the user's computer, including notice of significant effects of having the software or other similar technology installed. Marketers also must give the user an easy means to uninstall the technology and/or disable all functionality. Finally, marketers should always provide an easily accessible link to privacy policies and contact information, as well as clear identification of the company making the offer.

Given the rapid evolution of technology, DMA believes that self-regulation is the most effective means for setting business standards for legitimate marketing. Guidelines like those published by DMA and TRUSTe condemn deceptive practices, strive to protect consumers, and foster legitimate Internet advertising and marketing. Guidelines are flexible and adaptable to changes in markets, business practices, and advances in technology.

Another issue that DMA has sought to address through self-regulatory best practices is the role of advertisers in ensuring that their advertisements are being disseminated responsibly. In some instances, there may be advertisers with good intentions who do not understand where their ads are appearing online. To help address some of these issues, DMA adopted best practices regarding online advertising networks and affiliate marketing.⁸ These best practices state, among other things, that marketers should obtain assurances that their partners will comply with legal requirements and DMA's *Guidelines for Ethical Business Practice*, undertake due diligence in entering into these partnerships, define parameters for ad placement, and develop a monitoring system for online advertising and affiliate networks. These should limit the appearance of advertisements related to spyware.

⁸ See DMA Best Practices for Online Advertising Networks and Affiliate Marketing (attached) (available at <http://www.the-dma.org/guidelines/onlineadvertisingandaffiliatenetworkBP.pdf>).

ATTACHMENT 2

EXCERPT FROM THE DMA GUIDELINES FOR ETHICAL BUSINESS PRACTICE

Use of Software or Other Similar Technology Installed on a Computer or Similar Device*Article #40*

Marketers should not install, have installed, or use, software or other similar technology on a computer or similar device that initiates deceptive practices or interferes with a user's expectation of the functionality of the computer and its programs. Such practices include, but are not limited to, software or other similar technology that:

- Takes control of a computer (*e.g.*, relaying spam and viruses, modem hijacking, denial of service attacks, or endless loop pop-up advertisements)
- Deceptively modifies or deceptively disables security or browser settings or
- Prevents the user's efforts to disable or uninstall the software or other similar technology

Anyone that offers software or other similar technology that is installed on a computer or similar device for marketing purposes should:

- Give the computer user clear and conspicuous notice and choice at the point of joining a service or before the software or other similar technology begins operating on the user's computer, including notice of significant effects* of having the software or other similar technology installed
- Give the user an easy means to uninstall the software or other similar technology and/or disable all functionality
- Give an easily accessible link to your privacy policy and
- Give clear identification of the software or other similar technology's name and company information, and the ability for the user to contact that company

* Determination of whether there are significant effects includes, for example:

- Whether pop-up advertisements appear that are unexpected by the consumer
- Whether there are changes to the computer's home page or tool bar
- Whether there are any changes to settings in security software, such as a firewall, to permit the software to communicate with the marketer or the company deploying the software, or
- Whether there are any other operational results that would inhibit the user's expected functionality

Cookies or other passive means of data collection, including web beacons, are not governed by this Guideline. Article #37 provides guidance regarding cookies and other passive means of data collection.

ATTACHMENT 3

June 2006

DMA's Internet Marketing Advisory Board (IMAB) Best Practices for Online Advertising Networks and Affiliate Marketing

Online marketers using advertising and affiliate networks should:

1. Obtain assurances that the online advertising and affiliate network is in full compliance with state law, Federal law, and the DMA Guidelines for Ethical Business Practice.
2. Perform due diligence on prospective network advertising partners and make sure you are working with reputable firms. Additionally (if possible), obtain a sample list of current advertising clients. Due diligence should also include either: (1) asking for a full disclosure of eligible sites, or (2) a review of processes to limit access to unwanted sites or channels. When partnering with an aggregate site online advertising and affiliate networks should provide the marketer with a sampling of sites that are in their network. Due diligence should encompass the entire process from the marketer to the end consumer.
3. Always utilize a written contract/agreement. This will provide you the greatest possible control over your ad placement. This will also be the mechanism by which you devise and enforce formulas and/or guidelines for where and how online ads will be placed.

4. Include specific parameters that must be employed to determine placement of your online ads in written agreements. Altering of offer by an advertising or affiliate network is prohibited. If laws, guidelines or set standards are violated your contract with the violating advertising or affiliate network should be terminated.
5. Develop a system to routinely monitor your ad placements as well as your contract with any online advertising or affiliate network.

Senator NELSON. Mr. Rotenberg?

**STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR,
ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)**

Mr. ROTENBERG. Thank you very much, Senator, and thank you for the opportunity to testify today. The Electronic Privacy Information Center has a long-term interest in the ability of the Federal Trade Commission to police business practices that impact American consumers. We have worked with the FTC now for almost a decade to try to ensure that the Section 5 authority is used to protect consumers because if consumers do not have trust and confidence in the electronic marketplace clearly it's not good for consumers or businesses.

Of course, the concerns about spyware are very real and the costs are very real. For consumers it's not only their privacy and personal information, it's also the risk that financial details of bank account information, checking account information will be disclosed to others. It's the risk of identity thieves. It's the risk frankly simply of the hassle of having to monitor your personal computer to make sure that there's no improper surveillance taking place on your private activity.

So we see a real urgency in addressing the spyware issue and ensuring that the Federal Trade Commission has the authority, has the necessary tools to crack down on these activities.

Now, since you've asked us to make some brief remarks and because my full statement will be entered into the hearing record, I thought it might be helpful to place this bill a little bit in the context of where we've been and where I think we may be going. This bill addresses the specific problem of products, applications and techniques that are placed on the consumer's computer that surreptitiously take information from the user or exploit vulnerabilities on the computer's system.

Clearly these are bad practices. They should be prohibited. I think there are some changes that could be made in terms of scope and definition that might make the bill a little bit more effective. But I also think it's important to understand that this is simply one category of spyware and that there are other types of activities which I think you need to be aware of.

We have concerns, for example, about Internet service providers that now view the opportunity to intercept communications, the routine Internet traffic of their customers, for advertising purposes. From our perspective that's a form of spyware and if it's not addressed in this legislation perhaps it could be addressed somewhere else.

We're concerned about similar techniques that might be deployed against mobile telephones. A lot of information, personal information, is available on phones. These phones are becoming more so-

phisticated. They're essentially mobile computers and many of the same concerns about privacy protection and spyware exist there as well. Even the advertising techniques on social networking sites such as Facebook which make it possible for third party developers to get access to a lot of detailed personal information they don't really need access to is another issue we hope the Committee will consider.

Again, it may not be possible to get to all these issues with this legislation, and we do think this legislation is a step in the right direction. But I think it is important as the Committee thinks broadly about evolving business practices to be aware of these threats.

Now, to speak specifically about some of the recommendations that we would make for S. 1625, which we do favor—it's an important bill—we think it is clearly important to expand the FTC authority in this area so that when they do pursue these investigations we think it's important that the FTC authority not preempt State authority. We already have very important examples. In Washington State, for example, the State attorney general was able to go after a company that actually claimed it was offering a product to help people with spyware. The way it did it was to put up advertising on the user's computer which said: Oh, we've detected spyware on your computer; you need to purchase our product.

Well, the State attorney general was able to go after that company and reached a million dollar settlement. We think those types of innovative investigations and prosecutions are very important.

There is an issue with the exclusion for liability. A company under one provision in the bill would be given very broad authority to install spyware and we think that really needs to be reined in a bit and it is an exception. I don't think it's too difficult to deal with.

Finally, the category of information that the bill protects, what we think of as personally identifiable information, of course is changing very rapidly. Ten years ago we might have said, well, it's a person's telephone number and maybe their Social Security number. Now we need to think about their identity or user number on a Facebook or social networking service, because that's also a unique identifier that makes it possible to identify someone.

Even a person's password information, the person's Internet protocol address that's uniquely linked to a computer, is a type of personally identifiable information. We think those changes could be made in the bill as well.

But it is important legislation. It takes on part of the problem and I hope the Committee will be able to act favorably on it.

[The prepared statement of Mr. Rotenberg follows:]

PREPARED STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR,
ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)

Senator Pryor, Chairman Inouye, Senator Stevens and members of the Committee, thank you for the opportunity to testify today on the topic of spyware and S. 1625, the Counter Spy Act. My name is Marc Rotenberg and I am Executive Director of the Electronic Privacy Information Center. EPIC is a non-partisan research organization based in Washington, D.C. EPIC was founded in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amend-

ment, and constitutional values. EPIC recently filed a complaint at the Federal Trade Commission on the specific problem of commercial spyware.¹

Spyware, adware, and other information collection techniques are a growing threat to the privacy of Internet users. Computer users have noticed the effects. Ninety percent of users say they have adjusted their online behavior out of fear of falling victim to software intrusions.² The Webroot automated threat research tool has identified more than half a million different potential malware sites since January 2005.³ Spyware can cause significant degradation in system performance, result in loss of Internet access and impose substantial costs on consumers and businesses.⁴ Spyware can assert control over the operation of computers.⁵ The privacy risks of spyware include the theft of private information, monitoring of communications and tracking of an individual's online activity.⁶

Importantly, privacy threats are growing not just in numbers, but also in type. Traditional spyware, adware and tracking cookies are now joined by other threats such as mobile device spyware,⁷ "stalkerware," and the potential for social networking applications to function as spyware. Spyware comes from several sources including online attackers, organized crime, marketing organizations and trusted insiders.⁸

A new motivation for the cyber criminal is that spyware has become a profitable business.⁹ Individuals can also deploy spyware against each other.¹⁰ Some ISP's have also begun to install their own spyware-like services.¹¹

These threats require vigorous policy response. Policy must be able to innovate to recognize new challenges while substantively protecting consumer privacy.

Notice and Consent Schemes Do Not Adequately Protect User Information

Ultimately, users must be able to control how and when information about them is used, disclosed and held. Solutions which rely on simple notice and consent will not adequately protect users. A recent survey of California consumers showed that they fundamentally misunderstand their online privacy rights.¹² In two separate surveys almost 60 percent of consumers incorrectly believed that the presence of "privacy policy" meant that their privacy was protected.¹³ In a different survey, 55 percent of participants incorrectly believed that the presence of a privacy policy meant that websites could not sell their address and purchase information.

Users also routinely click through notices. The Pew Internet and American Life Project found that 73 percent of users do not always read agreements, privacy statements or other disclaimers before downloading or installing programs.¹⁴ In such an environment, merely giving notice to users before the collection of sensitive information from their computers fails to adequately protect privacy in the way consumers expect.

Consumer data should instead receive substantive protection. Information should be kept securely, and users should have the ability to know what data about them is being kept, who it has been shared with, and to withdraw consent for the holding of this data. Further, data should only be collected and kept for specified purposes.

Important security information should also receive protection, even if it does not identify a user. The Counter Spy Act places conditions on software that collects information such as the user's Social Security number and driver's license number. It also protects as "sensitive personal information" information such as financial account numbers when combined with passwords or other security codes.¹⁵ Password and access information to other accounts, such as e-mail or social networking, are not included.

EPIC recommends that strict protection be afforded to security information, such as username/password pairs, encryption keys, biometric data, or other access control information. The mining of this information may not lead directly to identity theft and other financial harm, but facilitates its spread. Gaining access to a user's non-financial accounts allows further information to be collected and further crimes perpetrated. Compromised accounts may have valuable information stored in them or be used to originate further malware attacks, including by impersonating the compromised account.

Privacy Requires Strong and Innovative Enforcement

EPIC supports giving the FTC the ability to seek treble fines and penalize pattern or practice violations, as section 7 of the Counter Spy Act does. These changes will improve the FTC's effectiveness in pursuing repeat offenders, and also change the economic incentives and disincentives for purveyors of spyware.

Several states are using innovative policies to protect their citizens' privacy. Spyware legislation has been passed in several states, including Alaska,¹⁶ Arizona,¹⁷ California,¹⁸ Florida,¹⁹ Georgia,²⁰ Illinois,²¹ Indiana,²² Iowa,²³ Louisiana,²⁴ Nevada,²⁵ New Hampshire,²⁶ Rhode Island,²⁷ Texas,²⁸ Utah,²⁹ and Washington.³⁰

The Utah statute, for example, makes provision for a private cause of action which may be brought by a mark owner who does business in Utah and is directly and adversely affected by the violation.³¹ In such a suit a mark owner may recover the greater of \$500 per each ad displayed or actual damages.³²

State Attorneys General have pursued spyware providers under state spyware laws. Washington State successfully applied the Washington State Computer Spyware Act³³ (Spyware Act) to stop Secure Computer's use of their free computer scan that always detects spyware leading to instructions to buy their Spyware Cleaner product in a \$1,000,000 settlement.³⁴ The State alleged violations under the state's Spyware Act, Federal and state spam laws, and the state Consumer Protection Act.³⁵ The Attorney General's Office accused the company of "falsely claiming computers were infected with spyware" to entice the consumer to pay for their program that claimed to remove it.³⁶ The settlement required the company to inform consumers of their right to a refund and pay a \$1,000,000 judgment.

For these reasons EPIC recommends that the Counter Spy act not preempt state laws and state enforcement actions, as section 11(b) does. Federal law should set a baseline of privacy protection. It should not cap it.

EPIC recommends that the limitation in section 6(a)(10) be removed. The Counter Spy Act's liability limitations broadly permit monitoring of users' computers and personal information for the "detection or prevention of the unauthorized use of software fraudulent or other illegal activities."³⁷ These limitations should be scaled back. The determination of whether uses are unauthorized, fraudulent or illegal may be complicated.

Privacy Threats Beyond Traditional Spyware Programs

Information collection online is not performed solely with spyware programs executed on user's computers. Third-party and opt-out cookies present growing threats. The proliferation of mobile devices means a potential new place for spyware to act. Internet service providers are begging to deploy their own adware and profiling services in ways which users will find difficult, if not impossible, to detect. Important user information is leaving the desktops and instead is residing on online social networking profiles. This information includes sensitive personal information such as contact information, one's social and business relationships, political interests, sexual orientation, as well as the contents of communications. Further, online social networking sites are increasing their own information collection practices.

A "cookie" is information about a particular user's identity and browsing behavior that web servers store on his computer, typically without his consent.³⁸ Cookies permit a user to customize his interface with a particular website, for example by automatically entering his username and password.³⁹ However, since cookies can match an individual user to his interests and browsing habits, they are increasingly placed, gathered, and exploited by advertisers and others with a commercial interest in precisely targeting ads and services.⁴⁰ Anyone with access to that user's cookies can track his browsing history and gather information about his behavior and identity.⁴¹ As a result, Internet users who are concerned about privacy are widely encouraged to routinely purge the cookies they have accumulated or to refuse cookies from websites that require them.⁴²

The recent Google/DoubleClick merger raises significant privacy issues because of the planned merger of the Google search engine database with Doubleclick's extensive data collection accomplished with third-party cookies.⁴³ EPIC filed a complaint with the FTC urging the Commission to impose privacy protections upon the merger, concluding:

Google's proposed acquisition of DoubleClick will give one company access to more information about the Internet activities of consumers than any other company in the world. Moreover, Google will operate with virtually no legal obligation to ensure the privacy, security, and accuracy of the personal data that it collects. At this time, there is simply no consumer privacy issue more pressing for the Commission to consider than Google's plan to combine the search histories and website visit records of Internet users.⁴⁴

In November 2007 Facebook launched its Beacon service.⁴⁵ Beacon collects information from Facebook users when engaged in actions on other websites. Facebook then uses this information to broadcast advertisements to that user's friends on Facebook, alerting them of the actions that the user took on these other websites. Initially, Facebook only provided a brief opportunity for an opt-out. Facebook later added an opt-in system, and the option to globally opt out of Beacon. Shortly after Beacon's launch, security researchers showed that Facebook is receiving information even from those who are not logged in to Facebook and are not Facebook members.⁴⁶

Users of social networking sites are also exposed to the information collection practices of third party social networking applications. On Facebook, installing applications grants this third party application provider access to nearly all of a user's information.⁴⁷ Significantly, third party applications do not only access the information about a given user that has added the application. Applications by default get access to much of the information about that user's friends and network members that the user can see. This level of access is often not necessary. Researchers at the University of Virginia found that 90 percent of applications are given more access privileges than they need.⁴⁸

These features may be exploited and the information used for other purposes. Investigators at the BBC took 3 hours to write an application that collected information that had been marked as unable to be shared with friends.⁴⁹ Facebook, as part of its response, cautioned that users should "employ the same precautions while downloading software from Facebook applications that they use when downloading software on their desktop."⁵⁰

Mobile device spyware also presents a future privacy threat, with unique features due to the mobile environment. In December 2006, McAfee reported on a new kind of mobile phone spyware, called SymbOS/Mobispy.A.⁵¹ SymbOS/Mobispy.A installed on phones and recorded incoming and outgoing SMS messages.⁵² It also tracked the phone numbers of all dialed and received calls. Mobile tracking presents unique dangers because it allows the tracker to determine the user's location. While the data may be able to follow users anonymously it may also easily identify them—they are likely at home in the evenings. Location information should receive significant protection from tracking applications.

A new more insidious form of adware has been tested in the United Kingdom, and at least one U.S. company has announced it will also use the system.⁵³ British Telecom contracted with the former adware company Phorm to create secret profiles of its users.⁵⁴ Users' traffic was routed via Phorm boxes, which replaced ads on the pages users were visiting with its own targeted ads. In the U.S., Charter communications announced that it will monitor consumers' browsing in order to serve them targeted ads.⁵⁵ Charter sent several of its users cryptic notices of an "enhancement" to their web browsing experiences.⁵⁶ The letter pointed users to a website with more details, including the claim that "[t]here is no application downloaded onto a user's computer and, therefore, there is no "adware" or "spyware" on your computer from Charter in this enhanced service."⁵⁷ Thus a system that is functionally equivalent to spyware, and more dangerous due to its undetectability, is touted as safer because it does not reside on the victim's computer.

Finally, some companies market spyware directly for consumers to use for stalking and other criminal activities. These technologies are promoted to consumers to spy on e-mail and instant message exchanges, record websites visited, and capture passwords and logins. EPIC has filed a complaint with the FTC against such "Stalker spyware," highlighting the unfair and deceptive practices used to market this software.⁵⁸ These practices include the promotion of illegal surveillance targets, the promotion of "Trojan Horse" e-mail attacks, and the failure to warn purchasers of the legal consequences of illegal use.

We hope the FTC will take action on this complaint and take action against these firms.

Conclusion

Privacy online continues to face many threats, both from criminal entities as well as intrusive commercial ventures. Substantive consumer protections and innovative enforcement strategies are necessary to protect consumers from the evolving threat of information collection online. These threats include not just traditional spyware, but also the merger of online consumer databases, new social networking features, mobile spyware and stalker spyware.

EPIC recommends passage of Counter Spy Act in line with the changes pointed out above. The Counter Spy Act should not preempt state law or enforcement; it should protect important security information like username/login pairs; and the liability limitations should be narrowed. Congress should also be aware of other developing threats to privacy beyond traditional spyware programs.

Footnotes

¹ Complaint, Request for Investigation, Injunction and Other Relief, *In the Matter of Awarenessstech.com, et al.*, (March 6, 2008), http://epic.org/privacy/dv/spy_software.pdf.

² Pew Internet & American Life Project, *Spyware: The Threat of Unwanted Software Programs is Changing the way People use the Internet*, 2 (July 2005), available at http://pewinternet.org/pdfs/PIP_Spyware_Report_July_05.pdf [hereinafter PEW Spyware Report].

³ Webroot, *State of Spyware Report Q2*, (2006), available at <http://www.webroot.com/pdf/2006-q2-sos-US.pdf>.

⁴Fed. Trade Comm'n, *Spyware Workshop—Monitoring Software on your PC: Spyware, Adware, and other software*, 8 (Mar. 2005) available at <http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf>.

⁵*Id.* at 9.

⁶*Id.*

⁷Joseph De Avila, *Do Hackers Pose a Threat to Smart Phones?*, THE WALL STREET JOURNAL, D1, May 27, 2008, available at http://online.wsj.com/article/SB121184343416921215.html?mod=todays_us_personal_journal.

⁸Aaron Hackworth USCERT, *Spyware*, 3 (2005) available at http://www.uscert.gov/reading_room/spyware.pdf.

⁹See Guillaume Lovet, *Dirty Money on the Wires: The Business Models of Cyber Criminals*, (2006), available at http://www.momindum.com/ressources/produits/fortuneFlash/content/libraries/_documents/index1/GL_Business_Models_of_Cybercriminals.pdf.

¹⁰EPIC, *Personal Surveillance Technologies* (May 2008), http://epic.org/privacy/dv/personal_surveillance.html.

¹¹Saul Hansell, *Charter Will Monitor Customer's Web Surfing to Target Ads*, THE NEW YORK TIMES, MAY 14, 2008, <http://bits.blogs.nytimes.com/2008/05/14/charter-will-monitor-customers-web-surfing-to-target-ads/>.

¹²Joseph Turow, Deirdre Mulligan, and Chris Jay Hoofnagle, *Consumers Fundamentally Misunderstand the Online Advertising Marketplace* (Oct. 2007), available at http://groups.ischool.berkeley.edu/samuelsonclinic/files/annenberg_samuelson_advertising.pdf.

¹³*Id.* at 1.

¹⁴Pew Spyware Report, *supra* note 2, at 6.

¹⁵S. 1625, 110th Cong. § 12(13)(B) (2008).

¹⁶Alaska Stat. §§ 45.45.792, 45.45.794, 45.45.798, 45.45.471 (2007).

¹⁷Ariz. Rev. Stat. § 44-7301 to -7304 (2008).

¹⁸Cal. Bus. & Prof. Code § 22947 (2008).

¹⁹Fla. Stat. § 934.02, .03, .06 (2008).

²⁰Ga. Code Ann. § 16-9-152, -157 (2008).

²¹720 Ill. Comp. Stat. 5/16D-3 (2008).

²²Ind. Code. § 24-4.8-1 to -3 (2008).

²³Iowa Code § 715 (2008).

²⁴La. Rev. Stat. Ann. § 51:2006-14 (2008).

²⁵Nev. Rev. Stat. Ann. § 205.4737 (2007).

²⁶N.H. Rev. Stat. Ann. § 359-H:1-6 (2008).

²⁷R.I. Gen. Laws § 11-52.2-7 (2008).

²⁸Tex. Bus. & Com. Code § 48.001-4, .051-057 (2008); Tex. Bus. & Com. Code § 324.001-7, .051-055, .101-102 (2008).

²⁹Utah Code Ann. § 13-40-101 to -401 (2008).

³⁰Wash. Rev. Code § 19.270.010-.080, .900 (2008).

³¹Utah Code Ann. § 13-40-301.

³²*Id.*

³³Wash. Rev. Code § 19.270.010-.080, .900.

³⁴*State of Washington v. Secure Computer, LLC*, No. C06-0126RSM (W.D. Wash. Nov. 30, 2006) (Consent Decree as to Defendants Secure Computer, LLC and Paul E. Burke), http://www.atg.wa.gov/uploadedFiles/Another/News/Press_Releases/2006/SecureComputerConsentDecree112906.pdf.

³⁵Press Release, Washington State Office of the Attorney General, Attorney General McKenna Announces \$1M Settlement in Washington's First Spyware Suit (Dec. 4, 2006), available at <http://www.atg.wa.gov/pressrelease.aspx?id=5926>.

³⁶*Id.*

³⁷S. 1625, 110th Cong. § 6(a)(10) (2008).

³⁸Cookiecentral.com, *The Cookie Concept*, http://www.cookiecentral.com/c_concept.htm (last visited June 6, 2008).

³⁹Cookiecentral.com, *Purpose of Cookies: The Cookie Controversy*, <http://www.cookiecentral.com/ccstory/cc2.htm> (last visited June 6, 2008).

⁴⁰*Id.*

⁴¹EPIC, *Cookies*, <http://epic.org/privacy/internet/cookies/>.

⁴²EPIC, *Does AskEraser Really Erase?*, <http://epic.org/privacy/ask/default.html>.

⁴³See EPIC, *Privacy? Proposed Google/DoubleClick Deal*, <http://epic.org/privacy/ftc/google/>

⁴⁴EPIC Complaint, *In the Matter of Google Inc. and DoubleClick Inc.*, 10 (April 20, 2007), http://epic.org/privacy/ftc/google/epic_complaint.pdf.

⁴⁵Facebook Beacon, <http://www.facebook.com/business/?beacon>.

⁴⁶CA Security Advisor, *Facebook's Misrepresentation of Beacon's Threat to Privacy: Tracking Users Who Opt Out or Are Not Logged In*, (Dec 3, 2007), <http://community.ca.com/blogs/securityadvisor/archive/2007/11/29/facebook-s-misrepresentation-of-beacon-s-threat-to-privacy-tracking-users-who-opt-out-or-are-not-logged-in.aspx>.

⁴⁷EPIC, *Facebook Privacy*, <http://epic.org/privacy/facebook/>.

⁴⁸Privacy Protection for Social Networking APIs, <http://www.cs.virginia.edu/felt/privacy/> (last visited June 6, 2008).

⁴⁹Press Release, BBC, *Facebook's loophole places personal profile data at risk—BBC investigation* (May 1, 2008), http://www.bbc.co.uk/pressoffice/pressreleases/stories/2008/05_may/01_click.shtml.

⁵⁰Q&A: *Facebook Response*, BBC, May 1, 2008, http://news.bbc.co.uk/2/hi/programmes/click_online/7375891.stm.

⁵¹McAfee Avert Labs Blog, <http://www.avertlabs.com/research/blog/?p=145> (last visited June 5, 2008).

⁵²*Id.*

⁵³ See EPIC, Deep Packet Inspection and Privacy, <http://epic.org/privacy/dpi/>.

⁵⁴ Chris Williams, *BT and Phorm secretly tracked 18,000 customers in 2006*, THE REGISTER, April 1, 2008, http://www.theregister.co.uk/2008/04/01/bt_phorm_2006m_trial/.

⁵⁵ Saul Hansell, *Charter Will Monitor Customers' Web Surfing to Target Ads*, THE NEW YORK TIMES, May 14, 2008, <http://bits.blogs.nytimes.com/2008/05/14/charter-will-monitor-customers-web-surfing-to-target-ads/>.

⁵⁶ Charter Letter, available at http://www.epic.org/privacy/dpi/subscriber_ltr.pdf.

⁵⁷ Charter Communications, Enhanced Online Experience Frequently Asked Questions, <http://connect.charter.com/landing/op1.html#6>.

⁵⁸ Complaint, Request for Investigation, Injunction and Other Relief, *In the Matter of Awarenessstech.com, et al.*, (March 6, 2008), http://epic.org/privacy/dv/spy_software.pdf.

Senator PRYOR [presiding]. Dr. Edelman?

**STATEMENT OF BENJAMIN G. EDELMAN,
ASSISTANT PROFESSOR, BUSINESS ADMINISTRATION,
HARVARD BUSINESS SCHOOL**

Dr. EDELMAN. Thank you, Senator Pryor, Senator Nelson, Members of the Committee.

Senator Pryor, I want to structure my remarks around your initial question about the proper definition of spyware and Senator Vitter's response immediately thereafter, concerned about both the risk of being over-inclusive and the risk of being under-inclusive, either of which would be a serious problem in making the legislation as effective as the Committee hopes.

I spend perhaps too much of my time in my lab testing spyware, going to the sorts of sites where users get infected, infecting my computer over and over, measuring the effects on it, figuring out how it gets infected and what it would take to clean the infections off. Well, two examples that I've seen in the past months I think are instructive for identifying potential under-inclusiveness of this legislation and then in rethinking alternative approaches that might help the Committee be that much more effective.

So here's one that I saw just 2 weeks ago in fact. A pop-up ad promised that it could, quote, "stop spam." Upon clicking on the pop-up, I received a long text, several hundred words, center-aligned. Part of the text was off screen. It was very hard to read, in short.

But if you read it carefully, you would find that it says it will show special offers in pop-up windows. OK, so it's saying it's going to show pop-up ads, but it's in a small font. The word "pop-up" is actually off-screen, so you'd have to scroll around to find it.

If you press "yes" the software will track the websites that you visit and the search terms that you enter and then, sure enough, it will show you pop-up ads, quite a few of them.

So what about that program vis à vis this legislation? Can you point to a clause of this legislation that that program violates? It's awfully hard to do actually. The program tracks some of the websites you visit, but when you look in Section 4, it needs to track those websites in a very particular way in order to fall afoul of that clause of Section 4. The underlying deception of having the tricky disclosure that's hard to read, you won't find anything about that in this legislation.

Here's another one: a program that tracks a user's name, street address, and all of the web searches that they do, then sends that to their server for a variety of purposes, market research, perhaps some kind of marketing. There too, it's hard to point to the clause in this legislation that the program violates. When you read

through the specific data elements that are prohibited under Section 4, you don't see the data that I listed that the program copies.

I think members of this committee would be concerned to have that sort of software on their computers, and would want it removed if they found it there and certainly the public shares that view, but it seems that this legislation wouldn't cover at least those two examples.

So what do we make of that? Well, Senator Pryor, as you and Senator Vitter immediately recognized, practices change quickly, and at our peril do we make a list of all the specific practices that ought to be prohibited, because the next day there will be more practices that we didn't think of, despite our best efforts.

So coming back to Ms. Harrington's remarks, I think she's absolutely right to emphasize the effectiveness on a long-term basis of the FTC Act. By prohibiting acts that have a tendency to deceive, that tend to be unfair to consumers—that is the sort of language that can prevent these one-sided bargains, where they show you pop-up ads and you don't get anything in return, or they track you in great detail without telling you. That is an approach that has lasted for decades and will serve us well going forward.

So what could this legislation do that would be helpful? Well, one, it seems the FTC lacks the statutory authority to get quite as large penalties as they ought to be able to receive. Imagine the settlement discussions between the FTC and a so-called adware maker. The adware maker is sitting there realizing that all the FTC can get is disgorgement of ill-gotten gains, and the company managed not to make a profit last year. So what's the disgorgement? The disgorgement is zero. How much of a penalty can the FTC really extract under those circumstances?

Consider a statutory grant of greater authority, of bigger penalties, of liquidated damages perhaps or some amount certain as a floor. "Even if you didn't manage to make money, well, we're going to make certain you lost money if you went around causing the kind of harm that's at issue." That could be very helpful. So I think that's an approach the Committee might want to consider, avoiding attempting to define spyware because we have enough of that under the FTC Act, but instead granting greater statutory protections in the form of increased liability.

My written remarks flag two other issues I hope the Committee will consider. For one, preemption of State law doesn't seem to me a good idea, given that there's more than enough work to go around to keep everyone busy and some innovative statutory approaches. Second, the Committee should avoid legislation that doesn't quite fill the field and makes it too easy for a vendor to claim to not be spyware. A vendor might claim: "We are federally certified good software; we passed Senator Pryor's standard and therefore we must be good." But in fact that vendor could still be pretty sneaky and could continue to cause users substantial harm.

So I'd caution the Committee at setting low standards. We need to be tough on spyware for the protection of all the users counting on this committee and this legislation for protection going forward.

Thank you for your interest in this matter.

[The prepared statement of Dr. Edelman follows:]

PREPARED STATEMENT OF BENJAMIN G. EDELMAN, ASSISTANT PROFESSOR,
HARVARD BUSINESS SCHOOL

Chairman Inouye, Senator Pryor, Members of the Committee:

My name is Benjamin Edelman. I am an Assistant Professor at the Harvard Business School, where my research focuses on the design of electronic marketplaces, including designing online marketplaces to assure safety, reliability, and efficiency. My full biography and publication list are at <http://www.benedelman.org/bio> and <http://www.benedelman.org/publications>.

Today the Committee considers the important problems of Internet spyware and deceptive adware—scourges that threaten the reliability, trustworthiness, and overall utility of many users' Internet's access.

My bottom line:

Despite some recent progress, spyware and adware continue to present substantial harms to Internet users and to the Internet as a whole.

Many improper practices are already prohibited under existing statutes including the FTC Act, state consumer protection statutes, and state anti-spyware legislation. These statutes have given rise to a series of cases, both public and private, that have somewhat reined in the problems of spyware and adware.

Tough Federal legislation could assist in bringing spyware and adware purveyors to justice, and in further deterring creation and support of this noxious software.

But the bill at hand addresses only a portion of the problem, while in some ways reducing the effectiveness of existing efforts. By prohibiting specific individual practices, the bill invites perpetrators to comply with the letter of the law while continuing to harm and deceive consumers. Moreover, perpetrators are likely to boast of compliance—despite offering software no reasonable user would want. These loopholes are inevitable in the bill's "laundry list" approach, which unavoidably omits deceptive schemes not yet invented.

Pages five and six set out my detailed suggestions for revision. I favor a rewrite that emphasizes consumer protection fundamentals such as a consumer's right to know what software runs on his PC, and to grant or deny consent to each program that asks to be installed. But the FTC has already established these principles through its existing anti-spyware litigation. Thanks to existing legislation plus the FTC's work to date, this bill can accomplish its apparent purpose without adding new prohibitions. Instead, this bill can grant the FTC discretion to seek increased penalties under existing statutes—sparing this committee the challenging task of deciding exactly what practices to prohibit.

The Consumer Victims of Spyware and Adware

Discussion of spyware and adware typically seeks, in the first instance, to attempt to protect the users who receive such software. After all, a computer with spyware or adware is often virtually crippled—filled with so many popups that doing other work is impossible or impractical, and slowed so dramatically that it is unappealing to use the computer for ordinary purposes. Legislation and enforcement can help prevent such damage.

Adware vendors often claim their software arrives on users' computers only after users agree. As a threshold matter, my hands-on testing has repeatedly proven that adware can become installed without a user's consent.¹ But even if a user did accept the software, adware popups can nonetheless present substantial concern. For example, some adware popups are sexually-explicit—sometimes appearing without any obvious way to close the resulting windows to remove the explicit images.² Other adware popups resort to deception to try to sell their wares—combining the interruption of popups with the trickery of false advertising.³ Moreover, adware popups appear separate from the programs that caused them—making it hard for users to understand where the ads came from, why they're there, and how to make them stop.

Users face a variety of costs in restoring a computer to good working order after an infection of spyware and/or adware. Some users hire technicians to make appropriate repairs. Others buy anti-spyware software. Furthermore, during the period

¹See e.g., "Who Profits from Security Holes?" <http://www.benedelman.org/news/111804-1.html>. See also "Nonconsensual 180 Installations Continue . . ." <http://www.benedelman.org/news/022006-1.html>. See also "Spyware Installation Methods." <http://www.benedelman.org/spyware/installations/>.

²"Spyware Showing Unrequested Sexually-Explicit Images." <http://www.benedelman.org/news/062206-1.html>.

³See e.g., "Zango Practices Violating Zango's Recent Settlement with the FTC" (heading "Zango Ads for Bogus Sites that Attempt to Defraud Users"). <http://www.benedelman.org/spyware/zango-violations/>.

in which spyware or adware impair a computer's operation, the user loses some or all access to the system he or she has paid for. These are real and troubling costs—out-of-pocket expense, lost time, and reduced productivity.

These harms are not outweighed by any countervailing benefits. Rare is the user who receives anything of genuine value from spyware or adware. Some vendors claim their software is useful, *e.g.*, letting a user “participate in a market research community” or “access premium content.” But these claims rarely survive scrutiny. For example, it is hard to see a *benefit* in being tracked for market research, when standard practice is to *pay* participants to allow their behavior to be tracked. Moreover, when a vendor promises “premium content” in exchange for popups, it turns out the supposed premium material is often readily available elsewhere for free, and/or material the vendor lacks proper license to redistribute.⁴

The harms caused by spyware and adware fall within the general realm of anti-consumer practices addressed by decades of consumer protection law. For example, just as other industries resorted to fine print to hide the unsavory aspects of their products,⁵ so too do adware vendors often turn to lengthy texts, scroll boxes, or euphemisms to “disclose” key effects of their software.⁶ Similarly, just as door-to-door salesmen made misleading claims to get consumers to let them in—literally, to “get a foot in the door”⁷—so too do adware vendors invoke deceptive campaigns to try to attract interest in their products.⁸ That the truth is (in some way) made known prior to purchase (or installation) is no defense: Once a vendor has resorted to deception, caselaw indicates that the deception cannot be cured through a (supposed) corrective disclosure. Legislation ought to consider these myriad deceptive practices—including anticipating that practices will continue to change as tricksters find new ways to deceive unsuspecting users.

The Deeper Problem: Imposing Negative Externalities on Others

In my view, spyware and adware legislation should also consider the substantial negative externalities that such programs impose on others.

For example, spyware and adware impose large costs on ISPs, computer makers, and software developers. In practice, users often turn to their ISPs and/or computer makers for assistance with problems caused by spyware and adware. Meanwhile, independent software makers must consider how their software interacts with spyware or adware unexpectedly on a user's computer—adding additional complexity and unpredictability.

Spyware and adware cause further harm to the Internet's infrastructure and to Internet users generally—even users who are not themselves infected with spyware or adware. As much as half of spam now comes from “zombie” infections.⁹ Even if you keep your computer clean, others may not—and their computers may be used to send you spam.

Furthermore, spyware and adware often attempt to defraud online advertisers—typically by claiming to show ads that were never actually shown, or by showing ads that users never agreed to receive. My research has uncovered spyware and adware performing click fraud—automatically activating pay-per-click advertisement links where advertisers are only supposed to pay if a user specifically and intentionally clicks such links.¹⁰ Spyware and adware even interfere with advertising strategies widely perceived to present a lower risk of fraud. For example, some advertisers pay advertising commissions only upon a user's purchase—protecting against click fraud.¹¹ But pay-per-purchase advertisers can nonetheless be tricked by spyware and adware. For example, spyware and adware popups sometimes claim commissions on purchases they actually did nothing to facilitate.¹²

⁴See *e.g.*, “Debunking Zango's ‘Content Economy.’” <http://www.benedelman.org/news/052808-1.html>.

⁵See *e.g.*, *Häagen-Dazs Co.*, 119 F.T.C. 762 (1995) (challenging effectiveness of fine-print footnote modifying “98 percent fat free” claim for frozen yogurt products that were not low in fat).

⁶See *e.g.*, “Gator's EULA Gone Bad.” <http://www.benedelman.org/news/112904-1.html>.

⁷See *e.g.*, *Encyclopedia Britannica*, 87 F.T.C. 421 (1976), *aff'd*, 605 P.2d 964 (7th Cir. 1979), *cert. denied*, 445 U.S. 934 (1980) (rejecting “deceptive door opener” sales pitches).

⁸See *e.g.*, “Zango Practices Violating Zango's Recent Settlement with the FTC” (heading “Widespread Zango Banner-Based Installations without Unavoidable, Prominent Disclosure of Material Terms (XP SP2)”) (*supra*).

⁹Xie *et al.*, “How Dynamic Are IP Addresses?” <http://research.microsoft.com/projects/sgps/sigcomm2007.pdf>.

¹⁰“The Spyware—Click-Fraud Connection.” <http://www.benedelman.org/news/040406-1.html>.

¹¹These pay-per-purchase advertising systems are also known as cost-per-acquisition or “CPA.”

¹²See *e.g.*, “Spyware Still Cheating Merchants . . .” <http://www.benedelman.org/news/052107-1.html>.

In short, spyware and adware make the Internet a place where ISPs and computer makers incur unexpected costs they must ultimately pass back to customers; where even those who keep their computers safe nonetheless suffer from the infections that plague others; where advertisers cannot feel confident in the leads they pay to receive. The resulting costs make the Internet a weaker platform on which to do business, to all our detriment.

How to Stop the Problems of Spyware and Adware

Unlike the viruses of prior decades, spyware and adware tend to be created by business enterprises—groups that design this unwanted software, foist it onto users' computers, and reap the rewards. The appropriate response: Find the perpetrators and hold them accountable.

The past 4 years have brought considerable progress in identifying spyware and adware purveyors, and holding them accountable for what they have done. The New York Attorney General's office brought the first major case against a spyware vendor, Intermix, whose KeenValue, IncrediFind, and other programs were widely installed on users' computers without any consent at all, and also without meaningful, informed consent. Subsequent litigation has pursued a variety of other vendors, with cases brought by the FTC, the City of Los Angeles, and Attorneys General in New York, South Carolina, Texas, and Washington. Several class actions have also challenged nonconsensual and deceptive installations.¹³

The prospect of similar litigation has pushed some spyware and adware vendors to substantially cease operations. For example, in the face of litigation against several of its competitors, Manhattan-based eXact Advertising shut its "adware" business, thereby ceasing the nonconsensual installation of its software that had previously been so prevalent.

Yet litigation has not stopped the deceptive practices of all vendors. Consider the actions of Bellevue, Washington-based Zango, Inc. During an FTC investigation of its practices, Zango stopped its partners from placing its software on users' computers without first obtaining user consent. But despite its settlement with the FTC, Zango continues installations that are predicated on deception. For example, Zango continues to solicit installations via fake-user interface banner advertisements which deceptively masquerade as *bona fide* messages from software already on a user's computer.¹⁴ Moreover, despite a settlement requirement that every Zango advertisement be "clearly and prominently" identified with the name of the program that delivered that ad, some Zango advertising toolbars still lack the required label.¹⁵

More generally, experience and economic intuition confirm the need for *tough* litigation to adequately deter sophisticated corporate wrongdoers. At present, FTC actions typically seek disgorgement of ill-gotten gains. But effective deterrence requires a penalty that *exceeds* disgorgement, since investigation and litigation are less than certain. (Otherwise, a rational perpetrator would proceed in expectation of sometimes getting to keep the proceeds.) Experience shows inadequate deterrence to be a real problem. Consider the FTC's \$1.5 million settlement with DirectRevenue—letting the company's principals retain \$20 million of ill-gotten gains. As FTC Commissioner Leibowitz pointed out in his dissent to that settlement, spyware purveyors ought not reap windfalls from their deceit. To that end, I support the bill's granting of a fine of three times the amount otherwise available. (Sec. 7(b)(1).)

Increasingly, purveyors of spyware and adware are not major U.S. companies that investigators can easily locate. Instead, surviving vendors tend to reside abroad, or at least tend to attempt to hide their true location. Despite their far-flung location, these vendors sometimes cause even more harm than American counterparts—seemingly taking greater liberties with users' computers on the view that they are beyond prosecutorial reach. Legislation ought to seek to disrupt these businesses and limit the harm they cause. In my view, the most promising approach comes through financial investigations: Although they're off-shore, these vendors still want to make money, and their primary revenue sources remain U.S. advertisers and ad networks. The New York Attorney General has already pursued selected advertisers

¹³ See e.g., *Sotelo v. DirectRevenue LLC*, No. 05 C 2562 (N.D. Ill. Aug. 29, 2005).

¹⁴ See e.g., "Zango Practices Violating . . ." (heading "Widespread Zango Banner-Based Installations without Unavoidable, Prominent Disclosure of Material Terms (XP SP2)") (*supra*). More recent (May 2008) proof on file.

¹⁵ See e.g., "Zango Practices Violating Zango's Recent Settlement with the FTC" (heading "Unlabeled Ads—Toolbars, Desktop Icons, and Pop-Ups"). <http://www.benedelman.org/spyware/zango-violations/>. May 2008 proof on file.

that intentionally purchased large amounts of “adware” advertising.¹⁶ It would be little stretch to pursue advertisers and ad networks that intentionally fund remaining spyware vendors.

Specific Concerns in the Legislation at Hand

Let me now turn to S. 1625, my specific suggestions, and some areas of concern.

S. 1625 Risks Setting Low Standards that Do Little to Protect Against Remaining “Adware”

S. 1625 rightly prohibits a range of outrageous and extreme behaviors. For example, it would be hard to defend the “endless loop popups” prohibited by Sec. 3(1)(D).

But it is possible to skirt the bill’s prohibitions while causing consumers substantial harm and continuing the same practices traditionally associated with spyware and adware. Rather than showing so many popups that a user “cannot close the advertisements without turning off the computer” (Sec. 3(1)(D)), a program might show one popup per minute—still a substantial intrusion, yet nowhere proscribed by S. 1625 as it stands. Similarly, rather than tracking the specific information prohibited under Sec. 4(a), a program might monitor “only” a user’s name, street address, phone number, and all web searches conducted. Although remarkably intrusive, such tracking is seemingly permitted under Sec. 4. Thus, S. 1625’s approach creates a serious risk that spyware and adware vendors can continue business substantially as usual.

Moreover, spyware and adware vendors are likely to attempt to use any Federal legislation as a “shield” to deflect criticism of their practices. Indeed, Zango already invokes its settlement with the FTC as a supposed indicator of endorsement. Last year, Zango staff wrote to security vendors to say Zango has received “certification with the FTC.”¹⁷ More recently, Zango claimed that security vendors ought not block or remove Zango software because if Zango’s software were harmful, “the FTC would not have entered into a consent agreement permitting Zango to market that software.”¹⁸ Far from setting a minimum standard that vendors will aspire to exceed, this bill thus risks creating a new supposed “certification” (or other low standard) that vendors may invoke as a defense against allegations of impropriety. As a result, weak legislation could actually make the spyware and adware problem *worse*.

Prohibiting the full spectrum of deceptive adware would require substantial reworking of S. 1625. Rather than prohibiting a lengthy list of specific bad acts, a rewrite would probably begin with basic consumer protection fundamentals, *e.g.*, that software must only be installed on a user’s computer after clear and prominent disclosure as well as meaningful consent.

If S. 1625 is to retain its present approach, a partially-responsive revision would add a preface or other comment to explicitly confirm the Committee’s intention—that compliance with S. 1625, in and of itself, does not assure that software is ethical, effective, desirable, or even useful. I realize that such an addition may seem vacuous—for of course the bill does not aspire to define what software is desirable or useful. But as the bill stands, adware vendors are virtually certain to attempt to invoke S. 1625 defensively—claiming that their software must be desirable since it meets the bill’s requirements. An appropriate preface could prevent that unwelcome strategy.

S. 1625 Should Protect Security Vendors Assisting Users

Security vendors face a barrage of complaints and, in some instances, litigation claiming that security firms err in removing harmful or deceptive software from users’ computers. See *e.g. Zango, Inc. v. Kaspersky Lab, Inc.* and *New.net v. Lavasoft*. Federal anti-spyware legislation offers a natural context in which to grant Good Samaritan protection to computer security software—immunizing the efforts of bona fide security vendors, in the ordinary course of business, to identify, block, and/or remove software users reasonably view as objectionable. S. 1625 could and should include such an immunization.

S. 1625 Should Not Preempt Tougher State Laws

As it stands, S. 1625 preempts tougher state laws. Given S. 1625’s limited prohibitions—a list of some specific bad acts, rather than a comprehensive framework for effective notice and consent—such preemption seems unwarranted.

¹⁶ Assurances of Discontinuance—Cingular, Priceline, Travelocity. <http://www.oag.state.ny.us/press/2007/jan/adware-scannedAODs.pdf>.

¹⁷ Forwarded e-mail on file in my possession.

¹⁸ Reply Brief of Appellant. *Zango, v. Kaspersky Lab*. U.S. Court of Appeals for the Ninth Circuit. No. 07–35800.

In particular, S. 1625 leaves ample room for states to do more to protect their consumers. For example, states could identify additional specific bad acts that ought not be permitted. Alternatively, states could identify alternative methods of enforcement—perhaps private litigation by those who are harmed (be they consumers, websites, computer makers, advertisers, ad networks, or otherwise). With so much room for innovation to further address these important problems, I see no proper basis for preemption of state legislation.

A Simplified Bill Could Increase Penalties while Avoiding Other Questions

A simplification of S. 1625 would strike all language except authorization of increased penalties. The treble fine in Sec. 7(b) would apply to all FTC actions under existing legislation, pertaining to software installed on a user's computer that tracks user characteristics or activities, or that shows advertising. This dramatic simplification would relieve the Committee from the challenging questions of what specific behaviors to prohibit, and would side-step all the concerns identified in my testimony. Yet this revision would offer major benefits—letting the FTC better sanction and deter perpetrators. I urge the Committee to consider this approach.

Senator PRYOR. Thank you.
Mr. Weafer?

**STATEMENT OF VINCENT WEAVER, VICE PRESIDENT,
SECURITY RESPONSE, SYMANTEC CORPORATION, ON BEHALF
OF THE BUSINESS SOFTWARE ALLIANCE (BSA)**

Mr. WEAVER. Mr. Chairman, Members of the Committee: Thank you very much for the opportunity to testify.

Let me start with a question that was raised earlier, which is how large is the problem. If we look at spyware and malicious code in general, there is about 1.8 million pieces of unique code. Now, that's a large number, but if you remember that about 800,000 of those malicious codes came in all of last year, so if you look at all the previous years last year represented the vast majority of those pieces of spyware and malicious code. In the first 6 months of this year, we've already surpassed what we saw last year, in 2007.

Looking another way, we did a survey of people's machines where we looked and we found about 57,000 unique pieces of files on their machine—Office, Windows, operating system files. 65 percent of those files were deemed to be potentially malicious or spyware on their machines.

The Organization for Economic Cooperation and Development has estimated that something like 95 million U.S. people are sitting with spyware on their machines. It's a large problem and it's still growing. Now, this includes not just the grey actors, but also the black actors, the criminalization that's occurring very much at the moment as well.

In terms of S. 1625, one of the areas we definitely want to focus on is on the focus of behavior, not technologies. So we certainly want to prohibit bad conduct rather than pick certain technologies and say this act is good or this is bad, because that frequently forms a low bar for companies that try and target or simply raise themselves to that minimum level and say: We're certified.

Second, we do want to include our support for the legislation, the so-called Good Samaritan portion. So a Federal court recently ruled in the *Kaspersky* case that the Communications Decency Act gives such protection to providers of anti-spyware solutions.

Now, we're not seeking unlimited protection. In fact, we believe the legislative codification of *Kaspersky* could include language requiring good faith as well as a fair and effective dispute resolution

process. There should be a process, it should be fair, it should be open. That's what we're looking for as part of this provision.

We also want to commend you for including in your bill a provision for allowing perfectly legitimate activities, such as the detection and prevention of unauthorized use of the software. This is essential to our industry, the software industry, because fraud or piracy also includes almost \$50 billion in damage every year. So we believe this is also an important part.

I'll keep my remarks short and just thank you very much for your time.

[The prepared statement of Mr. Weafer follows:]

PREPARED STATEMENT OF VINCENT WEAVER, VICE PRESIDENT, SECURITY RESPONSE, SYMANTEC CORPORATION ON BEHALF OF THE BUSINESS SOFTWARE ALLIANCE (BSA)

Mr. Chairman, Mr. Ranking Member, Members of the Committee, good afternoon. Thank you very much for the opportunity to testify here today. My name is Vincent Weafer and I am Vice President of Security Response at Symantec Corporation. I will be testifying today on behalf of the Business Software Alliance (BSA).

Symantec is one of the world's leading software companies. We are headquartered in Cupertino, California, operate in 40 countries worldwide and have more than 17,500 employees. Symantec's mission is to help individuals and enterprises assure the security, availability, and integrity of their electronic information. As the global leader in information security, we protect more people from online threats than anyone in the world. Symantec offers our customers products that detect and remove spyware and harmful adware, and our Norton brand of products is the worldwide leader in consumer security and problem-solving solutions.

The Business Software Alliance (www.bsa.org)¹ is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. Its members represent one of the fastest growing industries in the world. BSA programs foster technology innovation through education and policy initiatives that promote copyright protection, cyber security, trade and e-commerce.

It is a pleasure to be here today to discuss the serious issue of cyber security: protecting millions of computer users from those who maliciously install software on computers to compromise and steal sensitive, personal information. Such software goes by the name of "spyware." Mr. Chairman, I commend you and your colleagues, Senator Boxer and Senator Nelson for your leadership in addressing this invasive and deceptive practice through the Counter Spy Act (S. 1625).

Today, I would like to make three points:

First, spyware and harmful adware represent a critical threat to security and privacy on the Internet. It is a threat that must be met and defeated.

Second, legislation can and should play an important role. We urge the Committee to consider language which focuses on the malicious intent behind this reprehensible behavior, not "bad" technological tools like computers, software and the Internet. We want to work with you to ensure that anti-spyware legislation moving through Congress targets reprehensible behavior and avoids the trap of defining "good" or "bad" technology.

Third, we believe that legislation should contain specific provisions to ensure that developers of anti-spyware tools can protect their customers without fear of threats and legal harassment.

And *fourth*, we commend you for including in your bill a provision clarifying that security and anti-piracy activities are not in fact spyware.

What Threat Are We Facing?

Mr. Chairman, we commend you for your leadership in addressing the real threat and grave threat of spyware and harmful adware.

¹BSA members include Adobe, Apple, Autodesk, Avid, Bentley Systems, Borland, CA, Cadence Design Systems, Cisco Systems, CNC Software/Mastercam, Corel, Dell, EMC, HP, IBM, Intel, McAfee, Microsoft, Monotype Imaging, PTC, Quark, Quest Software, SAP, Siemens PLM Software, SolidWorks, Sybase, Symantec, Synopsys, and The MathWorks.

Spyware and harmful adware are stand-alone programs that can monitor system activity and either relay the information back to another computer or hold it for subsequent retrieval.

Spyware programs are placed on a user's system—often times without the knowledge of the user—in order to steal confidential information, such as usernames, passwords and credit card details. This can be done through keystroke logging, or capturing e-mail and instant messaging traffic. Spyware is of particular concern because of its potential for use in identity theft and fraud.

A growing type of spyware is rogue anti-spyware/anti-virus applications. They deceive users by displaying scary warnings about the computer being infected with a large number of fake threats, and then ask the user to buy the software to fix the problems. Another recent trend is programs that attempt to use the license agreement to prevent the end-user from sending any portion of the spyware program to anti-spyware companies.

Harmful adware programs capture information about the computer usage and Internet browsing habits of the user (such as websites visited and e-commerce purchases made). They generate a deluge of disruptive ads, usually in the form of pop-up windows, on the computer's screen. This represents a potential violation of privacy, and degrades user experience and computer performance by bogging down a computer's normal functions.

How prevalent is the problem of spyware and harmful adware?

Symantec publishes twice a year the Internet Security Threat Report (ISTR), a comprehensive compilation of Internet threat data, which gives us a unique perspective on the prevalence of spyware. The ISTR includes analysis of network-based attacks, a review of known vulnerabilities, and highlights of malicious code and additional security risks. We compile our data from more than 24,000 sensors monitoring network activity in over 180 countries, as well as information compiled from over 120 million client, server and gateway systems that have deployed our antivirus products, and through the 25 million e-mail messages we filter for our customers everyday.

According to our most recent Internet Security Threat Report, spyware continues to be a serious security risk for consumers. The latest Internet Security Threat Report released by Symantec in April 2008 reveals that Attackers have adopted stealth tactics that prey on end-users on individual computers via the World Wide Web, rather than attempting high-volume broadcast attacks to penetrate networks. This may be because enterprise network attacks are now more likely to be discovered and shut down, whereas specifically targeted malicious activity on end-user computers and/or websites is less likely to be detected. Site-specific vulnerabilities are perhaps the most telling indication of this trend. During the last 6 months of 2007, there were 11,253 site-specific cross-site scripting vulnerabilities = Cyber criminals continue to refine their attack methods in an attempt to remain undetected and to create global, cooperative networks to support the ongoing growth of criminal activity.

Adware and spyware continue to propagate, according to the ISTR. At the beginning of June 2008, there are over 1.8 million known malware and security risks with the majority of these being discovered in the past 18 months. In the last 6 months of 2007, threats to confidential information made up 68 percent of the volume of the top malicious code samples. Malicious code can expose confidential information in a variety of ways, including exporting user and system data, exporting e-mail addresses, recording keystrokes and allowing remote malicious access to a computer. At the same time, today's attacks are more surreptitious than ever before, less likely to be detected rapidly, and more likely to have a direct impact on a user's finances.

As an illustration of the scale of the problem, a recent report by the Organization for Economic Cooperation and Development (OECD), estimates that 59 million users in the U.S. have spyware or other types of malware on their computers.

In summary, spyware and harmful adware are, quite simply, a critical threat to our online security and privacy. It is wrong and it must be stopped.

Ban Bad Behavior, not Technology

Fortunately, the marketplace is responding to the need to address this challenge. Cyber security companies are investing heavily in newer generations of classification, behavioral detection and white listing technologies to handle the increasing volume and variety of spyware and malicious code threats. For example, Symantec creates security programs that watch out for known malicious threats, as well as unknown software that exhibits suspicious characteristics. Symantec products classify and categorize programs according to functionality. This allows a user to select an acceptable risk level and detect only programs that fall outside the user's own acceptable limits. We continually add new definitions and new defenses to address

the ever evolving dangers in the Internet threat landscape such as worms, spyware, spam, and phishing.

In addition, critical technologies such as web browsers are being revamped with more security, as they increasingly become a focus for attacks. Web browser security is particularly important because browsers come in contact with more untrusted or potentially hostile content than most other applications.

We believe however that, in addition to the response of the marketplace, legislation can and should play a role. Spyware is a serious online threat to the public interest. As you have recognized, Mr. Chairman, this threat requires Congress to empower Federal agencies to enforce prohibitions that will help curb the scourge of spyware and harmful adware.

We want to work with you to ensure that legislation moving through Congress targets reprehensible behavior, rather than attempts to define “good” or “bad” technology.

We believe that legislation should not prohibit specific technologies. Computers, software and the Internet are tools that are used in thousands of ways to enhance how we work, study, communicate and live. These tools are an indispensable part of our daily lives. The fact that a number of bad actors have figured out how to use these tools for illegitimate purposes does not mean the tools themselves are the cause of the harm.

If technology was to be constrained or regulated, we would lose much of the richness and power that computing has brought to our modern lives.

Let me put it a different way. We don’t ban crowbars because *some* people use them to break into houses. We don’t ban cars because *some* people use them to flee from the scene of a crime.

Prohibiting conduct, rather than technology, avoids the danger of dictating the design and operation of computer software and hardware. Congress has wisely avoided imposing a number of technology mandates to maintain the U.S. technology industry as the envy of the world. It has been responsible for incredible improvements in productivity, millions of jobs, billions of dollars in exports, and immense benefits to every consumer. Government intervention that replaces marketplace solutions with governmental decisions endangers America’s technology leadership. It hurts users of technology products by stifling innovation, freezing in place particular technologies, impairing product performance, and increasing consumer costs.

Mr. Chairman, Symantec and other BSA member companies want to work with you and your staff to ensure that S. 1625 focuses even more clearly on harmful activities, rather than on the technology that is misused to perform these activities.

Currently, S. 1625 includes a few provisions that risk affecting legitimate software and Internet functionalities, and thus compromise the operations of today’s computers—as well as the direction of future technology. Let me give you just a few examples:

- Section 3(1)(A) prohibits the installation of software that transmits or relays commercial electronic mail. This would constrain the development and use of legitimate and innovative methods to generate and send electronic communications;
- Section 3(3)(B) regulates how software that is installed on a computer must be named and where it must be located, and how it can be uninstalled. Again, this would constrain how legitimate software is deployed and operates.

We believe the problems inherent in such an approach can be avoided if Congress instead focuses directly on the behavior we are trying to stop: the use of unfair or deceptive means to install software on computers, as well as the unauthorized acquisition, use or commercialization of information from individuals. This is for example what section 2 and section 4(a) of your bill do. We commend you for the inclusion of such provisions, which strike at the heart of the spyware and harmful adware problem and which we believe would be useful tools in the hands of enforcement agencies.

Such an approach significantly mitigates the risk that legislation may hamper or constrain the development and use of technology, while achieving your objective of protecting computer users. In addition, while products can be moved offshore and out of reach of our laws, the collection of information from computers within our borders is a problem that we can more easily and effectively address.

Enable Anti-Spyware Companies to Continue to Best Protect Computer Users

Developers of anti-spyware solutions are providing effective protection to computer users against online threats. Unfortunately, they are threatened with lawsuits for defamation and interference with their business by spyware and harmful adware

companies. These spurious threats force anti-spyware companies to divert precious resources to fight to protect themselves in Court. This is intended to disrupt and deter the development of tools that empower consumers to stop unwanted software from being put on their computers.

BSA supports including in anti-spyware legislation what is often called a “Good Samaritan” provision. This would limit remedies against developers of anti-spyware tools. This would be far from unprecedented. In fact, Congress has repeatedly legislated targeted protection for a host of similarly beneficial activities, such as charitable food donations, the use of Automated External Defibrillators, or liability arising from sharing information about the Y2K problem.² Last but not least, in June of last year the House of Representatives supported, by an overwhelming majority of 368 to 48, H.R. 964, the Spy Act. The Spy Act includes such a Good Samaritan provision for anti-spyware activities.

Mr. Chairman, I want to bring to your attention an important Federal court case, *Zango v. Kaspersky*. In August 2007, the U.S. District Court for the Western District of Washington ruled that the protection afforded by section 230(c)(2) of the Communications Decency Act (CDA) of 1996 (47 U.S.C. 230), to providers of solutions that filter objectionable content, covers providers of anti-spyware solutions.³

Mr. Chairman, we understand why a former Attorney General like yourself would exercise caution in limiting judicial remedies. In fact, we are not seeking unlimited protection. We fully agree that good faith and due process *must* be applied by an anti-spyware provider when his product targets a software application for removal by the computer user.

We believe that the protection provided by Congress in section 230(c)(2) of the CDA can only extend to software providers who are truly seeking to empower users to exercise control over objectionable content received over the Internet. This protection does *not* apply if they are pursuing, for example, fraudulent or anti-competitive objectives (such as an anti-spyware company’s product blocking the installation of a competitor’s security solution.)

Mr. Chairman, BSA believes that legislative codification of the *Kaspersky* ruling, including language that requires good faith and fair and effective dispute resolution would in fact exceed the safeguards provided by the House when it passed H.R. 964 last year. It would thus provide a strong foundation for the Senate to work with the House toward enactment of legislation, which is a priority that BSA shares with you.

Security and Anti-Piracy Activities Are Not Spyware

Mr. Chairman, before I conclude my testimony, I would like to commend you for including in section 6(a) of your bill a provision allowing legitimate security and anti-piracy activities.

This exemption has been supported at the Federal and state levels by a host of technology industry organizations representing telecom providers, cable companies, software producers, and Internet service providers. The activities in question are perfectly legitimate, such as diagnostics, network or computer security, repairs, network management, etc. All these activities are conducted by network administrators to maintain and secure their systems.

Section 6(a) also covers the detection and prevention of the unauthorized use of software. This is essential to our industry’s ability to protect our products against theft. Software piracy results in almost \$50 billion in losses to the software industry each year, including more than \$8 billion in the U.S. alone. Given these massive losses, it is absolutely critical that companies that engage in otherwise lawful conduct to detect or prevent piracy or other unlawful acts are not unwittingly subject to liability under anti-spyware laws. Section 6(a) is narrowly and carefully drafted to address this important goal.

Certain interest groups may seek to drastically weaken or delete this provision. They may claim that it creates a license to snoop on people’s computers, shut down

²The Bill Emerson Good Samaritan Food Donation Act (42 U.S.C. 1791) precludes civil and criminal liability arising from food donated in good faith, except in cases of gross negligence or intentional misconduct. The Cardiac Arrest Survival Act of 2000 (42 U.S.C. 238q) precludes civil liability arising from any harm resulting from the use of an Automated External Defibrillator, except where there was no proper notification of emergency personnel, maintenance of the defibrillator or employee training. The Year 2000 Information and Readiness Disclosure Act (15 U.S.C. 1) precludes liability arising from statements and disclosures regarding the Y2K problem, except in cases of recklessness or intent to deceive.

³Zango has appealed the ruling and BSA, as well as several other online consumer protection organizations such as the AntiSpyware Coalition (ASC), the Center for Democracy and Technology (CDT) and the Electronic Frontier Foundation (EFF), have filed an Amicus Brief asking the Court of Appeals for the Ninth Circuit to affirm the District Court’s decision.

their IT networks, or circumvent state consumer protection, privacy, and contract laws. This is patently false. The provision does not go beyond limiting liability under your bill, and it limits liability under your bill only. Anyone who engages in an act that violates any other Federal or state law is and will remain fully liable under those laws. The purpose of weakening this provision is not to protect against spyware, but to make it harder for legitimate companies to fight piracy, or other fraudulent or illegal activities. The laudable anti-spyware goals of the Act should not be subverted for this purpose.

Thank you again for this opportunity to comment on the issue of spyware and the Counter Spy Act. I would be happy to answer any question you may have.

Senator PRYOR. Well, thank you.

Let me go ahead and start with you, Mr. Weafer, because I assume that your company has a working definition of spyware. Do you have a definition of spyware?

Mr. WEAFFER. Yes, we do.

Senator PRYOR. And as I understand it, the Federal Trade Commission does not have an adequate definition of spyware; is that right?

Mr. WEAFFER. That's right. There are different definitions out there. One thing we have done as an industry is come together to try and create a common definition of spyware. So we're part of a coalition, the Anti-Spyware Coalition. We have posted what we believe is a shared and fair assessment of what spyware is.

Even within that definition, there is some degree of what is included, what is considered personally identifiable information. We do believe there are fairly good standards relating to what is spyware and why the concern is there.

Senator PRYOR. So is there then an industry consensus on what spyware is and what it's not?

Mr. WEAFFER. We believe there is, even though there is probably some differences or subtleties in the language themselves.

Senator PRYOR. Do we have that definition? Have you provided that to the Committee?

Mr. WEAFFER. If we haven't, we will provide.

Senator PRYOR. That would be great because I think that would be helpful for us.

If I may, Mr. Edelman, it sounds like you spend a lot of time trying to figure out what's out there and you know how it infects people's computers and what it does. Tell me what you're seeing out there, two or three of the most prevalent forms of spyware that are currently infiltrating people's computers?

Dr. EDELMAN. Well, it's easy to be complacent and think that the problem of unwanted pop-up ads is over. That's not what I see in testing the sorts of websites where users get infected. I still see plenty of websites that will fill your computer with pop-ups and make money from those pop-ups through the biggest American ad networks out there. Maybe I shouldn't name any names today, but you can imagine the sort of advertising intermediaries who fund all kinds of behavior on the web and, remarkably, continue to fund the pop-ups that users so despise.

Separate from that, there are so-called market research companies that track users' behavior in great detail—every website you visit, every search you make, every product you buy, every product you look at but don't buy. That's a little spooky to me, frankly. I'm not sure I want those records about me kept anywhere. What if it

gets hacked? You know, what if that goes on the web somewhere and everyone can see it?

Beyond that, I do see serious criminal enterprises taking over users' computers, using them to send spam. I have to defend my computer so that when I allow my computer to be infected by spyware, it doesn't go around sending spam. So there's a little bit of complication even for me just in safely testing the software.

Denial of service attacks. Often you'll see programs that take over a user's computer and use it to attack some other computer.

All of these behaviors still remain prevalent, the same kinds of problems we were talking about 2 years ago, 3 years ago, 4 years ago still occurring, albeit some of them somewhat harder to track down.

Senator PRYOR. You mentioned that you go to the types of websites that will contain spyware. What types of websites typically expose people to spyware?

Dr. EDELMAN. Well, it can happen anywhere. You know, historically there have been examples even of mainstream news sites being hacked so that they would distribute spyware. But the sites that I find the most reliable tend to be second-tier entertainment sites. There's a wrestling site that is awfully effective at giving me spyware, with no offense intended to those who like professional wrestling, but this site isn't the one to go to. Again, I'll leave it unnamed.

Sites and programs that provide assistance in downloading copyrighted music and videos, sometimes massive copyright infringement frankly. You go to a site that purports to provide assistance in that regard and then you might or might not get the copyrighted material you were seeking, but in any event your computer would be destroyed, which certainly wasn't part of the bargain that you were expecting.

But again, it can happen anywhere and so we should not paint a picture of victims as somehow having brought this on themselves. Maybe in a few instances that's the case, but as a general rule that's really not true.

Senator PRYOR. Mr. Edelman, in your experience and in your opinion, is there any legitimate use for spyware?

Dr. EDELMAN. The programs that people call spyware are such a broad swath of programs, it's hard even to answer the question crisply. Is there any legitimate use for a program that takes over a user's computer and uses it to send unsolicited commercial e-mail to a variety of recipients who never asked for it, without telling the user that their computer would be so used? Absolutely not. How about a program that monitors what you're doing and shows pop-up ads? You know, some marketers say that that could be useful. You didn't know that American Airlines existed until you went to *United.com* and up came an ad for American Airlines, which, to be clear, they would never do because they are good advertisers and are actually very careful about that sort of thing.

In principle, it could be good for competition, I guess, to have pop-ups telling users about alternatives. But in practice I'm pretty suspicious. I think these pop-ups tend to promote software and services that users don't really want. If they want them they al-

ready know about them and no one wants to be interrupted by that sort of thing. So I don't see a lot of use for it.

Senator PRYOR. Mr. Cerasale, are there legitimate purposes, legitimate uses for spyware?

Mr. CERASALE. Well, again the term "spyware" means lots of things. Clearly, taking over someone's computer and so forth, is just not allowed. That's spyware, bad stuff. But certain toolbars, plug-ins, and web browsers, those types of things going on people's computers clearly are things that individuals want and so forth.

Looking at the definition of trying to be any kind of software, you even have requirements for e-mail notices. There are things called web beacons that are computer code, software code, to tell people whether or not an e-mail has been opened. Some of those things are used, for example, if there is a compelled e-mail notice to ensure that you have informed individuals of this notification. Those kinds of web beacons and things of that sort are definitely helpful and helpful to meet legal requirements.

So the definition—as you look at definition of what is spyware, and actually as you go down further, the definition of what is software, becomes very, very complicated. We have to be careful with that. If you look at the attachment to my testimony, the DMA Guidelines, we have a thing on the bottom, this does not include cookies or similar types of software, because we had difficulty trying to define this.

As we go further along with new technology, I think just defining software becomes a major problem. There are things that go on people's computers that can be easily defined as software, that are advantageous to them. Now, our guidelines would say you've got to allow me to take it off if I suddenly don't want it. But that's the kind of thing that we think is—there are some legitimate uses for.

There are major, major illegitimate uses for it that are already illegal. Many of the things that have been said here are already under Section 5 of the FTC Act, would be barred in its own right.

Senator PRYOR. Does the Direct Marketing Association have a good and working definition of spyware?

Mr. CERASALE. We do not. If you look at that, the attachment to my testimony, we just talk about computer software, "install software or other similar technology," because we don't know what's coming next, and then define some of the bad practices. So that's what we've done, and then defining if you're going to put this software or similar technology on someone's computer with notice, easy to uninstall, you have to let them know who it is and the privacy policy. That's the way we had to go. We felt that trying to define software would in essence—was first of all very difficult to try and discern; but technology is going to change the definition of software as we move forward, and we want to—and I think that our decision was to focus more on the acts and try and stop that, no matter what means was used for it.

Senator PRYOR. Mr. Butler, do you have a good working definition of spyware? Do you differentiate spyware from adware and other types of software?

Mr. BUTLER. To us, spyware is software that is surreptitiously installed on someone's computer, that allows the outsider to intercept or to seize even partial control over the user's interaction with

the computer, without that user's informed consent. Anything that meets that definition we think is spyware.

Senator PRYOR. Mr. Cerasale, you just heard his definition. You said the DMA doesn't differentiate between different types of software, but based on that definition you just heard, are you aware of any legitimate purpose for that type of software, surreptitiously installed, et cetera, et cetera, like he said?

Mr. CERASALE. As our guidance says, surreptitiously installed would violate our guidelines. So yes, that clearly fits within where DMA is. I think the one exception might be in an area where Mr. Butler and I would disagree, in areas of trying to look at anti-fraud areas, that that might be something where there may be an exception here. But not talking about that, looking at it from that score, his definition, surreptitiously put on, would violate our guidelines, so even without our definition.

Senator PRYOR. Let me ask this also if I may, Mr. Cerasale. That is, a couple of the witnesses either in their written testimony or what they said here today encouraged us to focus on behavior, not technology.

Mr. CERASALE. Correct.

Senator PRYOR. Is that where the direct marketers are as well?

Mr. CERASALE. I believe so, yes.

Senator PRYOR. Because the technology will change, but we know that the type behavior that we want to prevent, presumably we know the type of behavior we want to prevent, but the technology—there are lots of different ways to get there; is that fair?

Mr. CERASALE. That's fair, and it may be tomorrow it will be something new.

Senator PRYOR. Mr. Butler, do you agree with that?

Mr. BUTLER. I think so.

Senator PRYOR. Because I think what Senator Vitter said was that he was concerned about the definition and I think the idea, if I'm hearing the panel correctly, is that if you have a definition that's really based on a technology or a specific process of some sort, that could change because some programmer out there could change that tomorrow and the law we pass today could be obsolete. But if we focus on, I guess, the end result and the behavior that we're trying to prevent, then regardless of what technology gets us there, I think that gets us what we're trying to do.

Do you agree with that, Mr. Edelman?

Dr. EDELMAN. I think that's fine as far as it goes, but it's still possible to be both over-inclusive and under-inclusive as to behaviors. So it's possible to write a list of 20 bad behaviors and miss three other behaviors that either the Committee didn't notice or they haven't started yet, but will start next week.

Similarly, it's possible for there to be some behavior for which the behavior itself is neither good nor bad; it's the deceptive practice of that behavior, doing it in a way that has a tendency to deceive, based on the totality of the circumstances, the context, the method in which it is promoted, the nature of the disclosure, the nature of the consent procedure.

So the suggestion that behavior versus technology is the magic bullet that solves the bill's problems, I'm not sure it gets you all the way there.

Senator PRYOR. Mr. Rotenberg?

Mr. ROTENBERG. Senator, I've worked on quite a lot of privacy bills over the years and I just want to say I very much support your approach. By way of example, the Federal Privacy Act, the legislation that protects the privacy of citizens with respect to their records held by Federal agencies, was passed more than 30 years ago. It actually said almost nothing about technology. It spoke about the collection and use of personal data, who would have access to it, how you could obtain it, and what the penalties would be. It still works today.

By comparison, the privacy provisions in the Cable Communications Act of 1984, which are very good privacy provisions, was actually quite specific about the type of industry that would be covered. In 1984 there was a clear understanding of what the cable industry looked like, what interactive television looked like, and what privacy protection would require.

Well, today we have a great deal of interactive media, but those provisions from 1984 no longer apply because they were too technologically specific. So I think we need to focus on the activity, and of course I think it's possible by means of committee report or other means to give some examples. You can say with respect to current business practice, we want to prohibit surreptitious collection of a person's personal data without their consent, and an example might be, and then we can talk about some of the things that are taking place right now.

Senator PRYOR. Well, I would hope that all the panelists here would help us as we work on this bill and help us make sure we get it right, because, assuming the Senate passes this and the House passes it and the President signs it, we are trying to address this problem, and a wrong definition or a wrong section in the bill could totally undermine the purpose of what we're trying to do.

So I'd love to have all of you help us draft this. You all raise good points.

Let me ask, if I may, let me ask Mr. Weafer about the cost associated with a consumer having spyware on his computer and having to do something to get rid of that infection. What does it typically cost John Q. Public out there when he's on his computer? What does it typically cost him to get rid of the spyware once it has infected his computer?

Mr. WEAFFER. There is two parts to that answer. One is the actual physical damage, for example having to go in and remove pop-ups, unwanted software, which can range in terms of dollars from hundreds of dollars to thousands depending on how many machines, whether it's to be completely re-imaged, and who's doing the work.

The bigger, greater cost is really on the personal privacy. If data has been exposed or is assumed to be exposed, then the cost in terms of cleaning up their identity, their privacy, going after that, actually is very difficult to calculate. But I think that's the greater concern and the greater danger to a lot of users.

Senator PRYOR. Will a software product sold by Symantec stop spyware from being added in the first place or does it remove it once it's on there, or both?

Mr. WEAFFER. It tries to do both. So first of all, we're really just trying to give the tools to the end-users to identify what's on their machine. We classify according to large spyware, which is a general category of software, including actual spyware, remote access programs, tracking tools, hacking tools, and information, preventing them getting on. They're deemed to be high risk or low risk, to help the user. Then if they are on the system, helping them remove them from the system itself.

In some cases we can actually work with the vendors. If they've got a reasonable uninstaller, we can actually just call that and that becomes the uninstallation. For some of the more malicious, insidious programs, we have to do it ourselves.

Senator PRYOR. Symantec has a number of competitors out there that are offering spyware protection as well, right?

Mr. WEAFFER. That is correct.

Senator PRYOR. About how many are in that marketplace right now that are offering anti-spyware programs or software of some sort?

Mr. WEAFFER. There is at least 20 major vendors who are offering similar programs.

Senator PRYOR. Which ones are the best?

[Laughter.]

Mr. WEAFFER. Symantec. I'm a little bit biased toward the Norton brand.

Senator PRYOR. I just couldn't resist that one.

But nonetheless, there may be some ways for some computer users to get anti-spyware software free, but a lot of people have to pay for it as well. It kind of depends on your situation. So definitely there's a lot of cost associated with this, not just to the machine but also to your personal situation.

Mr. CERASALE, you said in your testimony that you think the industry—you prefer self-regulation, is that right?

Mr. CERASALE. That's correct.

Senator PRYOR. Well, when I hear the numbers of some of the statistics, I get the very distinct impression that self-regulation isn't working. So do you disagree with me on that?

Mr. CERASALE. I do. What we heard a lot of today and a lot of the statistics are basically criminal activity, activity that is deceptive, activity that already violates Section 5 of the Act or other criminal codes. Self-regulation requires law enforcement to stop criminal activities. Self-regulation is not there and cannot be there to prevent criminal activity.

I think the area we're looking at and the area that we're concerned in is going after the bad guys, the criminals, and being careful to protect the legitimate uses on the Internet that foster commerce. And I think in that arena self-regulation works well, for DMA members to have to follow our guidelines, the ability for us to quickly change guidelines, to take a look at new technologies when they come up. We have our own ethics procedure to go after and try and stop certain activities.

I think in that arena it works. It does not work in the criminal arena and we don't intend it to, and we want you to give the FTC as much money as they can to go out and try and enforce it.

Senator PRYOR. I do think one of the shortcomings of self-regulation is something you alluded to, and that is I think you have a lot of members who are acting responsibly and are out there trying to do the right thing and they're legitimate companies trying to be in this for the long term. But not all direct marketers are members of the DMA and a lot of them don't acknowledge or recognize or even consider your guidelines that you lay out.

So this may be one of those situations where the good actors out there may have to undergo some additional regulation to try to get the bad actors out of the marketplace.

Mr. CERASALE. We have supported legislation in the past, such as CAN-SPAM and in other areas, where we felt that self-regulation didn't work, and we pledge and have in the past and continue to work with you on this legislation, with you and the Committee on this legislation, and others in this area.

Our biggest concern is unintended consequences hurting legitimate business and that's where we want to work.

Senator PRYOR. Mr. Weafer, let me ask another question of you, and that is—we have heard some statistics today that are helpful, but I'm curious about, from your company's standpoint and just from your personal research and your experience, is spyware a growing problem? Is it becoming more prevalent or less prevalent?

Mr. WEAFFER. In my opinion, the broader aspect of spyware is actually becoming more prevalent. We're seeing more and more spyware. Now, most of this is driven by the underground economy. A lot of it is the criminalization of this. We're certainly seeing in many cases up to 500 percent year over year increases in the amount and variety of this type of spyware coming out.

We are continuing to see the shady commercialization as well, which are programs which are continuing to drive pop-ups, programs which are continuing to be fraudulent, programs which are still not giving users control, consent, and notification. So we do applaud the self-regulation, but we want to see additional remedies on top of that.

Senator PRYOR. Well, I agree with you. I think that that's what you're seeing out there. I just know really anecdotally from talking to people—just as an example, not too long ago I was talking to someone about their computer and they were getting all these pop-ups. They were getting a new toolbar, they were getting all this stuff, and they didn't know where it came from or how it came on there.

It's very frustrating for people. For most people, like for home use, your personal computer is your personal property and you don't want it to be infected and somehow damaged by other people, and certainly you don't want your personal information out there going to people that you don't want to have it.

So this is a serious problem. We do have this piece of legislation. All of you pointed out your thoughts on the legislation, even some of the shortcomings of the legislation. We appreciate that. We take all of that as constructive criticism.

What we're going to do is we're going to take our legislation, we're going to talk to the Members of the Committee, and we're going to see if we can help shape it and get it in the type of form where it's ready to move and move through the system. And hope-

fully some time in the next, I don't know, several months, maybe the next year, we'll have a very, very strong piece of legislation, very bipartisan, to try to make a big difference in the marketplace.

So I just want you to know you've been a very important part of this process and we appreciate you. Like I said, we definitely would appreciate your input as we go along, and always feel free to share your opinions or give us your insights because we don't claim the expertise here. We know who the experts are.

So with that, what I'm going to do is I'm going to adjourn the hearing here in just 1 minute. But first let me say that we're going to keep the record open and Senators may have additional questions or follow-up questions. So we'll get those to you and we'd love for you to get those back to us. We'll try to leave the record open for 2 weeks, so if you could get those back to us as quickly as you can.

Also, if there are documents—I think someone mentioned a study or some statistics or whatever it may be. If there are documents that you want to submit for the record, again the record will be open for 2 weeks and just get that to Committee staff and they'll distribute it as it should be.

So we appreciate your time, we appreciate you looking at the legislation, and we appreciate your being here today. With that, we're going to adjourn the hearing, and just say thank you.

[Whereupon, at 4:28 p.m., the hearing was adjourned.]

A P P E N D I X

TRUSTE

San Francisco, CA, June 24, 2008

Hon. MARK PRYOR,
Chairman,
Subcommittee on Consumer Affairs, Insurance, and Automotive Safety,
U.S. Senate,
Washington, DC.

Dear Chairman Pryor,

I am writing to respectfully request that this letter be added to the official record of the Senate Commerce Committee's hearing on June 11, 2008 entitled "The Impact and Policy Implications of Spyware on Consumers and Businesses."

I am the Vice President in charge of legal policy and compliance matters for TRUSTe. We are an independent, nonprofit organization with the mission of advancing privacy and trust for a networked world. Through long-term supportive relationships with our licensees, extensive interactions with consumers in our Watchdog Dispute Resolution program, and with the support and guidance of many established companies and industry experts, TRUSTe has earned a reputation as the leader in promoting privacy policy disclosures, informed user consent, and consumer education.

TRUSTe applauds the Committee's work on the issue of spyware. We have long articulated a public policy for privacy protection that incorporates the strength of government oversight, the discipline of industry self-governance, and the innovation of privacy-enhancing technology.

In his testimony before the Committee on June 11, Jerry Cerasale, senior vice president of government affairs for the Direct Marketing Association, referenced the self regulatory work underway to develop standards for downloadable software. He spoke of the work that TRUSTe has undertaken to develop a program of best practices. I would like to tell the Committee a little more about our Trusted Download Program.

TRUSTe has partnered with major online consumer portals and other industry leaders to develop the Trusted Download Program, a standards and a certification program for downloadable consumer desktop applications.

Program objectives:

- Empower consumers to make informed decisions.
- Establish the leading industry-wide standards for developers of downloadable applications.
- Identify and elevate trustworthy consumer applications for distributors and marketers.
- Protect the valued brands of online advertisers by enabling them to know which applications are trustworthy and which are not.

The Trusted Download Program certification combines strict standards, thorough review, ongoing monitoring, enforcement mechanisms and powerful market incentives.

The Program elevates those applications that meet the certification requirements through a whitelist, thereby providing consumer portals and other businesses a tool to distinguish responsible software applications. For downloadable desktop software developers, the program provides guidance on responsible behavior. A Trusted Download Seal at the point of download allows consumers to recognize applications that provide improved disclosures, more explicit control mechanisms, easier uninstall, and more respect for their personal information.

Trusted Download Sponsors and Advisory Committee Members are CNET download.com, Microsoft, Yahoo!, and the Center for Democracy and Technology (CDT).

Incentives for Compliance

TRUSTe serves a “whitelist” of certified applications to advertisers, distributors, consumer portals and other interested parties. In a market where the conduct of partners can be as important as the conduct of your own organization, businesses are turning to TRUSTe to help determine which applications they want to be affiliated with. The Program’s whitelist is regularly used to influence decisionmaking in advertising buys, bundling and distribution opportunities, and to resolve errant blacklistings.

The whitelist, provides an economic incentive for software providers to achieve and maintain certification. In addition, the Trusted Download Seal at the point of download reassures consumers and increases downloads, providing a direct economic benefit to software developers.

Scope

While there are exceptions, the program is aimed at consumer downloadable desktop software applications. It does not cover software downloaded exclusively to handheld devices (*i.e.*, mobile phones). While there are additional specific requirements for advertising and tracking software, many requirements also apply to all consumer downloadable applications. Advertising and tracking software providers will likely need to significantly change current practices to earn certification. In addition, the program will provide standards for all applications to offer consumers enhanced disclosures, easier uninstall and other benefits.

Certification

Application providers submit to TRUSTe a contract and a completed questionnaire including questions about how the application is distributed. TRUSTe conducts a thorough evaluation of the downloadable applications against the program standards to ensure they do not involve activities that are prohibited by the Program. Additional compliance assurance is being provided by AppLabs, a third party software testing lab that will evaluate the application’s relay of information and interaction with the recipient’s operating system.

Key Program Elements

The Program outlines certain requirements for all software and specifies additional requirements for advertising and tracking software. This approach ensures that the Program addresses practices that historically have created consumer confusion and anxiety. However, all software must meet specific program requirements and is tested for monitoring, relays, and behaviors that have historically been considered deceptive.

Notice

The Program imposes a layered approach, via a primary notice and reference notices such as the End User License Agreement, EULA, and the privacy statement. The primary notice must explain functionalities that impact the consumer experience and must be unavoidable, to ensure that users understand what they are downloading. EULAs and “opt-out” mechanisms are insufficient for providing such notice or obtaining consent. For example, unavoidable notice of any material changes to certain specified consumer settings is required for all software. Further, all ads delivered in certified advertising software must be labeled, and unavoidable notice of certain ad features must be provided.

Consent to Install is Required

Consumers must be offered notice and an opportunity to consent that is described in plain language and is as prominently displayed as the option to not install, Consent to install may not be obtained with a pre-selected option.

Easy Uninstall

Instructions for uninstallation must be easy to find and easy to understand, and methods for uninstalling must be available in places where consumers are accustomed to finding them, such as the Add/Remove Programs feature in the Windows Control Panel, or the Add-On management menus in browsers for browser Add-Ons. Uninstallation must remove all software associated with the particular application being uninstalled (with a few specific exceptions carved out in the Program Requirements), and cannot be contingent on a consumer’s providing Personally Identifiable Information, unless that information is required for account verification.

Prohibited Activities

No company can have an application certified if any of its applications exhibits a behavior listed in the Program’s Prohibited Activities section.

Examples of prohibited activities include:

- Taking control of a consumer's computer.
- Modifying security or other settings of the computer to cause damage or harm.
- Spyware tactics for surveillance and tracking, such as keystroke logging.
- Preventing reasonable efforts to block installation or to uninstall.
- Allowing a certified application to be bundled with any application currently engaging in any of the prohibited activities.

Special Protections for Children

Companies in the Program must prevent the distribution of their advertising or tracking software on children's websites—including by prohibiting their distribution partners and affiliates from such distribution.

Affiliate Controls

Since many advertising and tracking applications are distributed through second and third-party affiliates and/or bundled with other programs; relationships must be disclosed in attestations. Certified software is subject to random testing on instances found wherever an individual might encounter them.

Prior Behavior

The Program includes provisional certification for companies that have previously engaged in prohibited activities or other behaviors that call into question the Participant's ability to comply with the Program Requirements on an ongoing basis. In order to be certified, these companies will be subject to additional oversight including enhanced monitoring and a requirement to go back to all users who downloaded an uncertified version of the software application and obtain their opt-in consent.

Segregated Ad Inventory

Companies in the Program must maintain segregated ad inventory in certified versus uncertified applications. The application provider must be able to serve ads to users from whom consent was obtained versus users from whom consent has not been acceptably obtained.

Monitoring

Certified applications are monitored by TRUSTe for ongoing compliance with the Program's strict standards. A company risks termination from the program if any one of its certified applications violates the standards.

Enforcement

If monitoring uncovers suspected non-compliance, an application, or in some cases all of a company's applications, will be subjected to enforcement procedures by TRUSTe. Depending on severity and the results of a TRUSTe investigation, an application may be temporarily suspended or permanently removed from the program whitelist. In certain cases, a company or application may be terminated from the Program and the fact of its termination made public.

I have attached a copy* of the Trusted Download Program certification requirements to this letter and request that it also be included in the Committee's spyware hearing record.

TRUSTe appreciates your work in this area and would be pleased to serve as a resource should you or your staff have any questions. If you have any questions, please do not hesitate to contact me.

Sincerely,

JOHN P. TOMASZEWSKI, Esq.
Vice President, Legal, Policy & Compliance.

*This document is retained in the Committee files.

AMERICANS FOR FAIR ELECTRONIC COMMERCE TRANSACTIONS (AFFECT)

June 25, 2008

Hon. MARK PRYOR,
U.S. Senate Committee on Commerce, Science, and Transportation,
Washington, DC.

RE: FOLLOW-UP COMMENTS FOR THE RECORD OF THE HEARING ON THE "IMPACT
AND POLICY IMPLICATIONS OF SPYWARE ON CONSUMERS AND BUSINESSES"

Dear Senator Pryor:

Thank you for the opportunity to submit additional comments on behalf of AFFECT (Americans for Fair Electronic Commerce Transactions) on the impact and policy implications of spyware on consumers and businesses and on the Counter Spy Act (S. 1625).

As I stated in my testimony during the June 11, 2008 hearing, AFFECT is concerned about the exception section of the Counter Spy Act, Section 6(a). That section says that the list of prohibited acts in Sections 3, 4, and 5 of the bill "do not apply to any monitoring of or interaction with, a subscriber's Internet or other network connection or service, or a protected computer, by or at the direction of a telecommunications carrier, cable operator, computer hardware or software provider, financial institution or provider of information services or interactive computer service . . ."

These entities have immunity under the Counter Spy Act when what they're doing is done for a number of innocuous-sounding purposes. The first nine of these liability exemptions include network or computer security, diagnostics, technical support, repair, network management, authorized updates of software or system firmware, authorized remote system management, authorized provision of protection for users of the computer from objectionable content, and authorized scanning for computer software used in violation of sections 3, 4, or 5 for removal by an authorized user.

As I said at the hearing, AFFECT sees no legitimate reason why any of these nine activities would need an exemption from the actions prohibited by the bill because:

- none of them justifies an outside entity in installing zombies, engaging in modern hijacking for the purpose of causing damage to the computer or causing the authorized user to incur unauthorized financial charges, causing a denial of service attack for the purpose of causing damage, causing endless loop pop-up ads (Section 3(1));
- none of them justifies an outside entity in modifying an authorized user's security settings for the purpose of stealing the user's sensitive personal information, or disabling security settings for the purpose of causing damage to the computer or another computer, or through unfair or deceptive means modifying browser settings (Section 3(2));
- none of them justifies, without authorization, an outside entity in preventing a user's reasonable efforts to block installation, to disable, or to uninstall software by unfair or deceptive means (Section 3(3));
- none of them justifies an outsider in installing software that collects sensitive personal information from an authorized computer user without that user's informed consent, logs keystrokes, collects and correlates personal information with a history of websites visited, extracts the substantive contents of files or communications, or prevents an authorized user from uninstalling or disabling software (Section 4); and,
- none of them justifies an outsider in installing adware that conceals its operation (Section 5).

An exemption from the prohibited activities listed in the bill is simply not needed to allow or protect any legitimate activity.

AFFECT is particularly concerned about Subsection 6(a)(10). That tenth and final exemption would be granted when the otherwise prohibited acts are done for: "detection or prevention of the unauthorized use of software fraudulent or other illegal activities." The troubling questions raised by 6(a)(10) were pointed out in my written testimony, namely that the exemption would allow a software vendor to surreptitiously download code onto a user's computer and freely violate their privacy. It would allow the provider to set itself up as an ad hoc police force to conduct warrantless searches and to act as judge and jury to conduct unilateral seizures. Private entities *do not* and *should not* have the right to conduct law enforcement activities.

More troubling is the fact that the language of Subsection 6(a)(10) would effectively allow a software provider to unilaterally decide to remotely shut down the

user's computer or Internet or other network connection or service. But whether the use of a particular software is "unauthorized," "fraudulent," or "illegal" is often subject to legitimate dispute and merits some judicial consideration before a provider is allowed to unilaterally employ a drastic remedy like remote disablement.

In his written testimony, Vincent Weafer, the Symantec vice president who was representing the Business Software Alliance (BSA) at the hearing, praised Section 6(a)(10) as "essential to our industry's ability to protect our products against theft. Software piracy results in almost \$50 billion in losses to the software industry each year, including more than \$8 billion in the U.S. alone. Given these massive losses, it is absolutely critical that companies that engage in otherwise lawful conduct to detect or prevent piracy or other unlawful acts are not unwittingly subject to liability under anti-spyware laws."

Contrary to Mr. Wearer's statement, exemption from the prohibited actions listed in the bill is neither essential to a software vendor's legitimate efforts to protect against piracy, nor is it essential to protect legitimate activities from liability under the bill. Software vendors have a variety of legal remedies to attack piracy. If a software contract, for example, an End User License Agreement (EULA), is breached, the vendor would have the right to sue and collect damages. It could seek an injunction against further use. In addition, statutes, like the U.S. Copyright Act, or international copyright laws, may grant other rights and remedies, including access to Federal court and statutory damages, perhaps even enforcement by the FBI. In addition, the BSA itself is a well-known and very effective enforcement arm of the software industry.

Further, there is no reason the software industry can't employ technological approaches to combating piracy without remotely accessing software resident on the user's computer and unilaterally shutting it down. For example, the agreement between the software vendor and the user could clearly provide for a limited period of use and a "time bomb" built into the software that disables its operation at the expiration of the named period of time. The parties then could agree that the period of limited use could be renewed by the user obtaining a "key" from the vendor or sending a "validation" to continue the use.

It is not necessary to reach into a user's computer, to poll the machine, extract data, and phone home. It is not necessary to build in a "backdoor" which will make the computer vulnerable to exploitation by spies, hackers, saboteurs, or terrorists. And, there is no legitimate reason why a software vendor, network provider, or other outside entity should be allowed to unilaterally decide to remotely shut down the user's computer or Internet or other network connection or service. At a minimum, a software vendor who thinks it has not been paid, should be required to give notice, an opportunity to cure, and obtain a court order before employing remote disablement.

The Business Software Alliance appears to want to use Section 6 of your bill to gain the approval of policymakers for their use of electronic self-help. The fact of the matter is that this is an anti-spyware bill, not a bill designed to address tools for dealing with piracy.

During the hearing on June 11, you specifically asked for suggestions about how to define spyware. AFFECT offered the following definition: Spyware is computer software that is surreptitiously installed on a computer that allows an outsider to intercept or take partial control over the user's interaction with the computer, without the user's informed consent. We believe this definition is broad enough to cover technologies that are deployed without appropriate user consent or are implemented in ways that impair user control over material changes that affect their experience, privacy, or system security; their use of their system resources, including what software is installed on their computers; and the collection, use, and distribution of their personal or other sensitive information. We also believe it should cover all of the prohibited behaviors currently listed in the bill.

AFFECT also sees the merit in the suggestions of spyware expert Ben Edelman, who advocated for a simplification of the approach of S. 1625 that would focus on increasing the penalties such as a treble fine in FTC actions. That approach was also expressed by the FTC in its testimony.

Finally, I want to express AFFECT's support for the three key principles expressed by Ms. Eileen Harrington, Deputy Director of the Bureau of Consumer Protection of the FTC, in her written and oral statements: (1) a consumer's computer belongs to him or her, not to the software distributor, and it must be the consumer's choice whether or not to install software; (2) burying in an End User License Agreement (EULA) material disclosures necessary to correct an otherwise misleading impression should not be sufficient to allow a spyware purveyor to escape liability; and (3) a consumer should be able to uninstall or disable any program he or she does not want on a computer.

AFFECT has long favored a competitive and fair marketplace. A cornerstone of AFFECT's efforts was the creation of "12 Principles for Fair Commerce in Software and Other Digital Products" (<http://www.ucita.com/pdf/AFFECTbrochure2-05.pdf>). Two of those key principles are that: (1) customers are entitled to control their own computer systems; and (2) customers are entitled to control their own data. We believe these two principles are consistent with the three expressed by Ms. Harrington and should guide the Committee and the Congress in shaping its approach to dealing with the insidious problem of spyware.

Thank you very much for the opportunity to submit these additional comments for the hearing record. AFFECT remains willing and interested in working with the Committee on S. 1625 and will be glad to be of whatever help we can.

Sincerely,

ARTHUR A. BUTLER,
Attorney, Ater Wynne LLP.

AMERICANS FOR FAIR ELECTRONIC COMMERCE TRANSACTIONS (AFFECT) CONCERNS
WITH S. 1625, SECTION 6(A)(10)

Americans for Fair Electronic Commerce Transactions (AFFECT) is a national coalition of consumers, retail and manufacturing businesses, insurance institutions, financial institutions, technology professionals and librarians committed to promoting the growth of fair and competitive commerce in software and other digital products.

S. 1625 (Pryor), introduced in June 2007, would protect against the unauthorized installation of software that is used to take control of a computer in order to cause damage, collect personal information without consent, or otherwise enable identity theft.

AFFECT strongly supports S. 1625's purpose to curb the use of harmful spyware. However, it has great concerns with S. 1625 (6), the exception section, which is overly broad and could be construed to protect wrongful acts that can result in great harm to computer users—which is in direct opposition to the purpose of S. 1625.

AFFECT strongly recommends that the exception provision of S. 1625 should *only* limit liability for interaction with a network, service, or computer that is undertaken to detect or prevent fraudulent or other illegal activities *as prohibited by the act itself*. Therefore, AFFECT proposes that Section 6(a)(10) of the bill be amended as follows:

(10) detection or prevention of fraudulent or other illegal activities *as prohibited by this Act*.

Subsection 6(a)(10), as it is currently written, would permit a provider to monitor or interact with an individual's computer or Internet or other network connection or service for the "detection or prevention of the unauthorized use of software for fraudulent or other illegal activities." This would allow the provider to unilaterally decide to remotely shut down the user's computer or Internet or other network connection or service. But whether the use of a particular software is "unauthorized," "fraudulent," or "illegal" is often subject to legitimate dispute and merits some judicial consideration before a provider is allowed to unilaterally employ a drastic remedy like remote disablement.

Permitting unilateral remote disablement is bad public policy. It allows the provider to set itself up as an ad hoc police force to conduct warrantless searches and to act as judge and jury to conduct unilateral seizures in the name of protecting against piracy, fraud, or other illegal activities. Private entities do not and should not have the right to conduct law enforcement activities.

Also, remote disablement can cause great harm to the owner who depends on access to and use of that computer, connection or service.

- For example, the shutdown of an owner's system can cause great harm to:
 - a teacher using a computer to prepare for classroom lectures;
 - an insurer depending on a computer system to pay claims;
 - a manufacturer trying to deliver its products to meet contractual commitments; or
 - the public's access to online library materials.
- In reaching into an individual's computer remotely to disable software residing on his computer, the provider may not only violate privacy rights, but also damage his other files.

- The monitoring and remote disablement of software on an owner's computer by a provider may compromise private information of employees, confidential and proprietary information of the owner, and, in some cases, national security information.
- The code used to remotely enter a computer and disable the software or the network connection (often called "black holes") make the computer vulnerable to security breaches by hackers and terrorists. When there is an opportunity to negotiate, many enterprises, including governmental entities, will insist that their software license agreements contain a warranty prohibiting any "self-help code" or other software routing designed to disable a computer program automatically or that is under the positive control of a person other than the licensee of the software. Unfortunately, with mass market licenses individual consumers and businesses are not able to negotiate for a "no self-help code."

It is important to recognize that these harms that can result from permitting remote disablement can be significantly larger than the harm to a software vendor in not getting a license fee.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAVID VITTER TO
EILEEN HARRINGTON¹

Question 1. Who do you think would define "objectionable" in S. 1625 section 6(a)(8), and what does that term mean?

Answer. The term "objectionable content" is left undefined by the Counter Spy Act, S. 1625. Absent a clear definition in the bill, "objectionable content" will need to be interpreted by the courts. As drafted, however, "objectionable content" is sufficiently broad that it might include content or software (such as advertising software, toolbars, etc.) about whose value reasonable people may disagree. Accordingly, a covered party could have considerable discretion under the bill to identify and remove software as "objectionable" without giving specific notice to, and perhaps against the intentions of, the consumer.

Question 2. Under section 6(a)(9) of S. 1625, would a consumer's purchase and use of a computer with pre-loaded operating system and anti-spyware software be sufficient "authorization" to allow some software to remove or disable other software on the computer without notifying the computer user or obtaining her consent?

Answer. The Commission and the courts would need to approach scenarios like the one posed by Question 2 on a case-by-case basis, weighing the nature of the software and its potential for harm against the nature and timing of notice and consent—if any—provided. In the case of pre-installed anti-spyware software, we would need to know how much notice the consumer is given regarding the existence and function of the software, and whether the consumer is given notice before the anti-spyware software removes or disables other software on the computer. If any pre-installed software caused the type of harms outlined in sections 3, 4, or 5 of S. 1625, it is doubtful that the Commission would deem the mere acts of buying and turning on a computer to be sufficient "authorization."

Linking exemptions and immunity in section 6(a) to particular functions that are purportedly "authorized" poses the risk of creating a safe harbor based on unknowing authorization. For example, a software provider, an information services provider, or an ISP might argue that a provision buried deep in an End User License Agreement or privacy policy provides sufficient authorization for much of the conduct prohibited by the bill.

Question 3. Should we be careful when providing (broad) exemptions or immunity for software removal, given the FTC actions against companies that might represent their software as legitimate "anti-spyware" in order to scam consumers?

Answer. Yes. I share Senator Vitter's concern that there is a need for caution in providing broad exemptions and immunity for software removal when addressing the problems of spyware. If not carefully drafted, these broad exemptions can create safe harbor loopholes that can be exploited by clever spyware and malware purveyors. Under the bill as drafted, virtually any "software provider" or "provider of information services" who can muster some plausible pretense of the list of the enumerated services will raise the exemption as a defense to enforcement.

Take the example of a purveyor of what has been termed "rogue anti-spyware" software. Rogue anti-spyware software is usually sold via deceptive tactics. A broad

¹As with my responses to the Committee's questions at the hearing, these answers present my personal views and do not necessarily represent the views of the Federal Trade Commission or of any Commissioner.

“anti-spyware” exemption may shield the rogue anti-spyware sellers from liability for their deceptive tactics. Moreover, it could potentially permit the seller to download other harmful software, such as a keylogger, if that seller can convince a court that the other harmful software in any way could be used to provide functions enumerated by sections 6(a)(1) through (10).

If the main purpose of including section 6(a) is to limit liability among and between civil litigants regarding questions about what is “authorized,” or what is “objectionable” (*e.g.*, where an anti-spyware company is sued by a software provider whose product is deemed objectionable), it is misplaced because S. 1625 does not provide a private right of action. Accordingly, such broad exemptions from law enforcement in this legislation are unnecessary. At bottom, the broad scope of section 6(a)’s limitations on liability—both in terms of the number of exempted parties as well as the breadth of the exempted conduct—may make the FTC’s job more challenging and potentially do more harm than good in terms of effective spyware law enforcement.

