BEFORE THE

SENATE COMMERCE COMMITTEE

HEARING ON

THE IMPACT AND POLICY IMPLICATIONS OF SPYWARE ON CONSUMERS AND BUSINESSES AND S. 1625, THE COUNTER SPY ACT

JUNE 11, 2008

TESTIMONY OF

JERRY CERASALE
SENIOR VICE PRESIDENT, GOVERNMENT AFFAIRS

ON BEHALF OF

DIRECT MARKETING ASSOCIATION, INC.

Jerry Cerasale
Senior Vice President, Government Affairs
Direct Marketing Association, Inc.
1615 L Street, NW Suite 1100
Washington, DC 20036
202/955-5030

I. Introduction & 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% 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% from the 1st quarter of 2007. The Census Bureau also noted that 1st quarter e-commerce sales accounted for 3.4% 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.

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 three years has limited pernicious software downloads, reducing spyware's threat to the positive consumer experience online. Together, we

---

[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.

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

[4] Use 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).

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

---

[5] *See, 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).

[6] CFAA, 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.

[7] For 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 Direct Revenue, http://www.oag.state.ny.us/press/2006/apr/apr04a_06.html.

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.

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).

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.

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.

June 2006