

BEFORE THE
SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION
OF THE
HOUSE ENERGY & COMMERCE COMMITTEE

HEARING ON
COMBATING SPYWARE: H.R. 964, THE SPY ACT

MARCH 15, 2007

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 Subcommittee. 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 Subcommittee as it examines H.R. 964 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 continued outreach to the business community on this important issue. I note at the outset that this is a complicated issue; there is no panacea that can fully solve it. In part due to the Committee’s attention, over the past two years there have been significant developments that have fundamentally improved the consumer experience as it relates to spyware. Where once, just two short years ago, pop-up ads, drive-by downloads, and software that hijacked computers were on the rise, consumers in 2007 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, we do not believe that a broad regulatory approach to all software downloads and Internet marketing as set forth in Section 3 of this bill is the appropriate approach to this issue and is not in the best interest of either consumers or business.

DMA is particularly concerned that this legislation could negatively impact legitimate advertisers and marketing practices that are critical drivers of the Internet economy. Internet growth over the past 10 years has been nothing short of remarkable, and this growth is fueled by advertising and marketing. The dramatic rise of the Internet is evident in the dollar amounts consumers spend purchasing products through Internet sales. This year, on Cyber Monday, nearly 30 million shoppers spent more than \$608 million in just one day. The numbers are up 26% from the same day last year and are more than the amount shoppers spent on Black Friday.

The U.S. Census Bureau, which releases quarterly retail e-commerce statistics, recently reported that estimated retail e-commerce sales for the 4th quarter of 2006 were \$29.3 billion, an increase of 6.3% from the 3rd quarter of 2006, and an increase of 24.6 percent from the 4th quarter of 2005. It also noted that 4th quarter e-commerce sales accounted for 3.0% of total sales.¹ comScore Networks reported that for calendar year 2006, online retail spending reached \$102.1 billion, a 24% increase from 2005.²

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 two years has limited pernicious software downloads. Specifically, spyware's threat to the positive consumer experience online has been reduced. Together, we are winning the battle against such malicious practices. This said, this battle will be ongoing. Today's solutions and remedies may be obsolete tomorrow. As technology

¹ U.S. Census Bureau. *Quarterly Retail E-commerce Sales, 4th Quarter 2006*, February 16, 2007. See <http://www.census.gov/mrts/www/data/html/06Q4.html>.

² See <http://www.comscore.com/press/release.asp?press=1166>.

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 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.³ In our experience, industry guidelines are the most effective way to address 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.

DMA requires member organizations to adhere to this Guideline, which encourages members to provide notice and choice regarding software that may be downloaded onto a consumer's personal computer or similar devices. The 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. The 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.

³ 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>).

The 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, about which you will hear today, 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, last year DMA adopted best practices regarding online advertising networks and affiliate marketing.⁴ These best practices state, among other things, that marketers should obtain assurances that their partners will comply with legal requirements and DMA's Ethical guidelines, 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.

B. Current Law Enforcement Efforts

Technology, self-regulation, and existing laws and enforcement are adequately addressing the problems caused by spyware. In the past couple of years, law enforcement

⁴ See DMA Best Practices for Online Advertising Networks and Affiliate Marketing (attached) (available at <http://www.the-dma.org/guidelines/onlineadvertisingandaffiliatenetworkBP.pdf>).

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, it 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 has 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. The Marketplace Technology Adopted 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 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, and other attorneys general, have been actively pursuing cases against companies for deceptive practices in connection with spyware and adware. See NY AG 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 H.R. 964

I would like to take this opportunity to describe specific comments regarding H.R. 964, which is pending before the Subcommittee. Although DMA is aware that similar legislation passed the House in each of the last two Congresses, we believe that the significant developments we described warrant reevaluation of certain provisions of this legislation, which we hope that the sponsors of this bill and the Subcommittee will consider.

First, DMA has significant concerns about Section 3 of the bill, and is concerned that it would limit current and future critical Internet offerings. For this reason, DMA believes that Section 3 should be tailored to target defined bad practices, rather than create regulation of many legitimate information practices resulting from software. The current language in Section 3 extends beyond regulating “surreptitious surveillance” practices and would apply notice and consent to all “information collection software,” defined to include software that collects personally identifiable information or non-identifiable information used for advertising purposes. DMA and its membership have long supported the principle of notice and choice surrounding the use of personally identifiable information. However, requiring notice and consent for all information practices tied to software downloads would result in limiting the consumer’s Internet experience. The proposed requirements would prove an obstacle to consumer personalization and customization of websites as consumers would eventually cancel requests to transmit information, without first learning of the program’s purpose, missing the opportunity to obtain unique and valuable tools that could enrich their online experiences. This would all culminate in a restraint on innovation and the deployment of new, seamless technologies.

DMA also is concerned about the possible consequences from a provider acting under the “Good Samaritan” protection in Section 5. This provision, unlike prior proposals, would limit liability for violations “under this Act” for providers of anti-spyware software that remove spyware from a computer. This provision is far narrower than previous proposals that would have limited liability for such providers for any removal of software.

The policy goal underlying the current Good Samaritan proposal is unclear. The operative provisions of Sections 2 and 3 would impose liability for placing software on a machine, not removing software. Thus, it is unclear why a provision limiting liability for

“removal” of software is necessary. If the Committee’s goal is to not impose liability on entities that place anti-spyware software on a computer, a more appropriate approach would be to exempt providers of such software from the definition of “information collection software” in the first instance. Given the circumstances surrounding this provision and the fact that it is limiting liability where none exists in the first instance, DMA suggests that the provision be removed.

Although DMA supports a provider’s ability to remove or disable a program employed to perpetrate a bad act, we are apprehensive that a broader “Good Samaritan” provision would empower providers to remove legitimate software from a customer’s computer and thus raises competitive concerns. Program removal can be a complex procedure with unintended negative effects, especially when the software cannot be isolated. A forced removal may cause other legitimate programs to improperly function or not function at all. In the end, the consumer would suffer. 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 of such programs and should be preserved.

Finally, DMA believes that Section 5(b), which provides immunity to the specified entities for monitoring undertaken for purposes including security and fraud detection and prevention, is drafted too narrowly and should be extended to cover the activities of entities beyond those enumerated that engage in fraud prevention activities. For example, DMA member companies, including information service providers acting on another company’s behalf (e.g., online retailer), are involved in financial transactions, such as extending credit. When a consumer applies for credit, these member companies provide critical fraud prevention tools that must operate seamlessly with the overall process. To isolate such an anti-fraud tool would undermine the overall security of the online transaction. For these reasons, Section 5(b) should be more broadly drafted to include other vital anti-fraud activities.

IV. Conclusion

In summary, the combination of advances in industry self-regulation, FTC enforcement, and technology, coupled with concerns about interfering with legitimate uses of software for marketing purposes, necessitates that Section 3 be revisited. If regulation is necessary, it should

be drafted in manner that does not undermine current efforts or upset consumers' expectations regarding the types of available, legitimate online marketing.

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

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