Prepared Testimony and
Statement for the Record of

Joseph Pasqua
Vice President of Research
Symantec Corporation

Hearing on

"'Do-Not-Track' Legislation: Is Now the Right Time?"

Before the

U.S. House of Representatives
Committee on Energy and Commerce
Subcommittee on Commerce, Trade, and Consumer Protection

December 2, 2010
2123 Rayburn House Office Building

Introduction

Chairman Rush, Ranking Member Whitfield, and Members of the Subcommittee, thank you for the opportunity to appear before you today as the Committee considers a national "Do-Not-Track" Registry as part of an overall effort to protect consumers' online privacy.

My name is Joe Pasqua and I am the Vice President of Research for Symantec Corporation[1]. I am responsible for all activities within Symantec Research Labs[2], the company's global research organization.

Symantec welcomes the opportunity to provide our insights to the Committee as Congress, the Federal Trade Commission, the Department of Commerce and others begin to explore the merits of new privacy initiatives and legislation designed to provide consumers with greater protection, transparency and control of their information in the online world.

Symantec supports Congress's objective of protecting privacy and enhancing consumer trust. As the global information security leader, Symantec has over 25 years of experience in developing Internet security technology. Our Symantec and Norton brands protect more than 370 million computers or email accounts worldwide. We specialize in protecting our customers' computers, networks, information and interactions as they work and play online. No one knows more about how to protect users, their families and their information than Symantec. In short, we protect more people from more online threats than anyone in the world.

Today, I would like the Committee to take away at least three key points:

First, online privacy is not possible without security. Through spyware and certain harmful adware, online advertising can present a critical threat to security, and therefore privacy on the Internet.

Second, while privacy legislation can and should help protect Americans in the online world, we urge the Committee to focus on malicious behavior rather than allegedly malicious tools such as devices or software. We want to work with you to ensure that privacy legislation targets reprehensible behavior and avoids the trap of defining "good" or "bad" technology – an exercise that could have the unintended consequence of undermining cybersecurity or stifling economic activity.

Third, while online privacy and security together are a critical foundation to trust on the Internet, the creation of a Do-Not-Track registry would be unlikely to advance these goals. Instead, Congress should focus on policies that foster an online environment where individuals and organizations can complete transactions with confidence, trusting each other's identities and the infrastructure on which the transactions run.

---

[1] Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.

[2] Symantec Research Labs (SRL) is Symantec's global research organization and has played a leading role in developing and commercializing numerous cutting-edge technologies across Symantec's business areas. Commercialized technologies from the group include industry leading rootkit protection, innovative browser protection technology to proactively block future exploits of known vulnerabilities, Symantec's first antispam technology, generic exploit blocking technology that proactively blocks fast-spreading threats, online consumer security services, and technology to help protect our nation's critical power-grid infrastructure. SRL also partners with outside organizations on joint projects, through its university and government research efforts.

No Privacy Without Security

As the world's largest internet security provider, we agree that online privacy is a cornerstone of consumer trust. Without security, however, the expense of compliance and lost economic activity from additional privacy regulations is hardly worth it. The lesson: deal with security first, and do not create impediments to security inadvertently through new privacy laws.

The advantages of doing business over the Internet are tremendous--but only if enterprises can ensure that exchanging information in cyberspace is secure. Interaction with Web sites increasingly demands personal information. Ordering products online requires personal shipping addresses and credit card information. Sharing data requires trusting business partners across open network architectures and relying on unknown data security infrastructures to complete transactions. When data and documents are transferred across poorly controlled networks and repositories of personal data are accumulated in hidden databases, the potential for corrupted information or compromised personal privacy increases. The integrity of business transaction records may become questionable, and individuals may become victims of identity theft or other fraud.

Clearly, security and privacy have become major issues for the Internet's personal and business users. The communications speed and document-management advantages of Internet use are tremendous, but these conveniences are diminished when users must proceed cautiously because of a lack of confidence in the robustness of security or real concerns about misuse of Internet-based information. Without security, additional privacy regulations will be ineffective in protecting individuals' ability to control their own information and will result in expensive formalities and lost economic activity.

The Evolving Online Advertising Business And Associated Threats

Online behavioral advertising is not inherently bad, but it does carry with it – sometimes literally – collateral threats to information security. Consider some of the overall trends related to Web advertising. First, the Web has exploded in popularity, and people are spending more and more time each day surfing their favorite sites. Second, online advertising has proven itself to be a viable business model for many companies. Countless Web sites are displaying more ads that are viewed by an ever greater number of people. Third, the online advertising supply chain is fairly complex. In the simplest incarnation, an advertiser might work with an ad network that will in turn arrange to have the ad published through one or more content publishers. In a more complex, but still quite common incarnation, an ad network might work with a syndicator and many sub-syndicators. Fourth, advertising itself has become very rich in content and applications. While text-based advertisements are still popular, we are seeing more elaborate ads that use technologies, such as Flash. The reality is that an online advertisement is more than just an ad – it is a small piece of software that runs on your machine in the context of your Web browser. And finally, browsers are becoming far more complex. In addition to the core Web browser, people often enhance their Web experience through one or more plug-ins. For example, Flash is enabled on a Web browser through a plug-in.

The increase in prevalence combined with the heightened complexity makes online advertising a ripe target for attackers. Because an advertisement is basically a piece of software, the potential exists for that software to be malicious. Symantec observed such a vulnerability in a popular social networking site in which one of the site's advertisements took advantage of a well known Windows vulnerability. More than one million people saw the advertisement. Although the vulnerability was known, and although a patch had been issued, it is likely that many people who viewed the ad did not have their patches up to date.

In such cases, a Web site that hosts advertising can be an otherwise innocent bystander; the advertisement content itself is provided by an ad network, not the host. What makes attacks leveraging online advertising especially powerful is that it is entirely possible for an otherwise trustworthy, popular, and well-meaning site to host an advertisement containing malicious code.

Also, the tools of the trade are fungible. Anything one can do in a scripting language like JavaScript can also be done in Flash. So, in principle, Flash-based advertisements can implement the same kinds of attacks that are possible through malicious JavaScript. These include scanning internal network hosts and "drive-by pharming." Cutting through the technical jargon, all of this means that an attack can be perpetrated with whatever tool, or advertising software, is available. The tool is neutral, the attacker is not.

Symantec expects the number of malicious online ads to grow. The unfortunate moral here is that there are no real safe locations on the Internet. That should not deter consumers from surfing the Web; but they must realize how important it is to be protected.

The Use Of Adware And Spyware

A whole class of threats commonly known as adware and spyware has proliferated over the last few years with very few impediments. These programs are security risks that typically are used to gather marketing information or display advertisements in order to generate revenue. Not only are these threats far more widespread than traditional malware, but also they use more advanced techniques. No doubt this is because adware and spyware programs are being created by registered corporations with professional developers rather than by hobbyist virus writers.

Spyware and adware programs are related, and in some cases their functionalities may overlap; additionally, they may have similar functionality to viruses and worms, such as displaying text or gathering information. However, one important difference from viruses and worms is that they lack the property of self-replication.

There are also key differences between spyware and adware. For example, while they both may collect information about you or your activities, the types of information they collect tends to differ. Spyware programs may log your keystrokes, capture your email and instant messaging traffic, or harvest your sensitive personal information such as passwords and login IDs, or credit card details. The compromised data is then sent on to someone else. Depending upon their intention, they may use the information however they wish; for example, accessing and controlling your system remotely, or running up charges using your credit card information. Identity theft can also be facilitated by spyware.

Spyware can be introduced into your computer system from any number of vectors; essentially, any source of executable code can become a vector for spyware transmission. However, some routes are more common than others. For example, consumers frequently download spyware without knowing it – typically attached to shareware or freeware, when they click on links in email messages or instant messaging clients, or even when they accept the conditions of fake anti-spyware software licensing agreements. In some cases, simply visiting a Web site can result in an automatic install of unwanted software. This technique is known as "drive-by downloading."

Adware, on the other hand, generally consists of components that work together to collect a different sort of personal information: the sites you visit, your browsing habits, and your apparent likes and dislikes. Adware then sends this data on to companies that have purchased the services of the adware provider to assist in

compilation of information on your personal preferences. This data can then be used to send tailor-made advertisements applicable to your interests. This data is typically not personally identifiable. It is also important to note that not all adware tracks behavior, but some simply displays advertisements to the end user through the program. While the risk posed by such applications is low, they can constitute a violation of organizational policy or introduce risk to the host system.

As with spyware, adware can be downloaded via the Web or by clicking on links in email messages or instant messaging clients. It is sometimes bundled with other software, and you may or may not be notified of its introduction onto your system. It is not uncommon for computers to have more than one type of spyware or adware installed; additionally, use of peer-to-peer file-sharing programs increases the risk of acquiring these programs. Finally, some adware and spyware adds a BHO (Browser Helper Object) to your system. A BHO is an add-on program that can add features to your browser. Loaded every time a browser is launched, a BHO can be used by adware and spyware for its own purposes.

Some programs classified as adware or spyware are commercially released programs that can be used in a variety of ways. In and of themselves, they are not malicious, but they can threaten your privacy or security, and the availability of your system. Because of these risks, some users may wish to be able to detect these programs. Thus, Symantec classifies programs based on a number of characteristics, including their potential impact on privacy, confidentiality, integrity, and system availability. Once categorized, they can be detected by Symantec's security products, and users can choose whether to keep or remove them based on their corporate or personal requirements.

How Prevalent Is The Problem Of Spyware And Harmful Adware?

How many spyware and adware programs are actually out there? How likely is it that these programs will impact your system? It is difficult to know exactly how much spyware and adware exists at any given time because the number is highly dynamic. However, various ways can be used to determine the programs that appear to be most prevalent and to assess the potential impact on users. Symantec publishes an annual Internet Security Threat Report[3], which is a comprehensive compilation of Internet threat data and provides a unique perspective on the prevalence of spyware. The Report includes an analysis of network-based attacks, a review of known vulnerabilities, and highlights of malicious code and other security risks. According to our most recent Report, spyware and adware continue to be a serious security risk for consumers.

The latest Report reveals that attackers have adopted stealth tactics that prey on end users on individual computers via "staged downloaders." These machines install malicious code onto a compromised computer and allow attackers to alter the downloadable component to any type of threat to suit their changing objectives over time. Setting aside the most common type of attack for a moment, the second most prevalent downloader component observed by Symantec in 2009 was the Sality.AE virus. Once installed, Sality.AE attempts to contact certain IP addresses to download and install its secondary components. One of the files it attempts to install is an adware program that periodically displays pop-up advertisements. If clicked, these ads generate income for the malicious code author and possibly the adware developer.

[3] Symantec's Internet Security Threat Report, Volume XV, April 2010. The Symantec Internet Security Threat Report provides an annual overview and detailed analysis of Internet threat activity, malicious code, and known vulnerabilities. The report also discusses trends in phishing, spam and observed activities on underground economy servers.

The Wimad Trojan147 was the third most common staged downloader component in 2009. This Trojan arrives on computers as a license-protected multimedia file. When the file is opened, Wimad exploits the intended functionality of digital rights management (DRM) technology in order to open a window and access an attacker-controlled URL. When an attacker's Web page is processed, a deceptive message is displayed that asks the user to click a button. If clicked, the Trojan downloads other threats, including adware and spyware.

As an illustration of the scale of the problem, a report by the Organisation for Economic Co-operation and Development[4], estimates that 59 million users in the U.S. have spyware or other types of malware on their computers.

Tracking Cookies Are Cause for Privacy Concern

Given the millions of threats that Symantec products block every day, you might find it interesting to know which detection consistently holds the top spot. It is not a worm such as W32.Stuxnet, a virus like W32.Virut, or even one of our long-term generic detections, such as Backdoor.Trojan. The detection most frequently encountered by Symantec antivirus users is tracking cookies.

Tracking cookies do what they say on the tin: they track your browsing habits. And while many types of cookies serve a useful purpose, and are used on most websites, tracking cookies can be considered a privacy concern. Some media companies that use them have found a way to resurrect deleted tracking cookies by using other cookies that are stored within Flash applications. These "Zombie cookies" can be detected by Symantec antivirus system scans, just as regular tracking cookies are, and can be removed from users' computers.

Social Engineering Banner Ads

The first challenge for adware and spyware vendors is to get people to install their software. Virus writers face exactly the same challenge and solve it by using social engineering techniques to entice users into running their creation. They use email messages with message bodies such as 'check out this message' and then attach their virus rather than legitimate content. Not surprisingly, similar techniques are used by adware and spyware vendors. Many websites use banner ad services. Unfortunately, many banner ads are completely misleading. Some banner ads use an image that mimics a Windows message box with an urgent message tricking computer users into clicking on the fake message box, then redirects the user to sites that initiate the installation of adware or spyware. Some of these fake message boxes will state the user's computer is infected or cite another system problem. When clicking the fake message box, the user is redirected to install software to correct the problem, when in fact the user was not infected.

Ban Bad Behavior, Not Technology

Fortunately, the marketplace is responding to the need to address the challenges of adware and spyware. 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 our part, Symantec creates security programs that watch out for known malicious threats, as well as unknown

[4] The Organisation for Economic Co-operation and Development (OECD), "*Malicious Software (Malware): A Security Threat to the Internet Economy*." June, 17, 2008.

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 un-trusted or potentially hostile content than most other applications.

Symantec has delivered a number of highly innovative new security technologies introduced in Norton Internet Security and Norton Anti-Virus 2010. Our new reputation-based security, named Quorum, leverages the wisdom of Norton's tens of millions of participating customers to derive highly accurate security ratings for virtually every file available on the Internet. This empowers Symantec users to make far better choices about the software they download and install on their computers. In addition, we introduced a new generation of heuristics to detect unknown malware files before they can run and cause damage. This advanced approach detects new malware, spyware and adware strains without known fingerprints, searching files for suspicious sequences of instructions typically used by malicious software. Finally, Symantec completely redesigned the behavioral protection, enabling it to recognize and block thousands of new malware variants by analyzing the behaviors of running software, all without known fingerprints.

We believe, however, that in addition to the response of the marketplace, legislation can and should play a role in protecting privacy online. 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. The fact that a number of bad actors have figured out how to use these tools for illegitimate purposes does not mean that 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 do not ban crowbars because some people use them to break into houses. We do not 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 technology mandates and the U.S. technology industry remains the envy of the world.

A "Do-Not-Track" List

Organizations including consumer, privacy, and technology groups have proposed the development of a "Do-Not-Track" list in hopes of providing consumers the ability to prevent advertising networks from being able to track the websites consumers are visiting. The proposed "Do-Not-Track" list is modeled in large part on the idea of the "Do Not Call" list that the Federal Trade Commission implemented in 2003 with significant success.

Conceptually, the idea seems reasonable, but in practice it would be an extremely difficult, if not unrealistic technical task.

In order to abide by an instruction not to track, a Web site must have a way to recognize that a given user connecting to that site has requested that they not be tracked. This recognition could be accomplished by identifying the user such that the user's registered tracking preference can be retrieved from a do-not-track list (e.g., a database). Because it is analogous to using phone numbers to identify a do not call list, consideration has been given to using IP addresses to recognize a connecting user. However, this approach is quite

problematic, as it requires that a user register all of the IP addresses from which they may connect. Given that users have an ever increasing array of Internet connected devices such as desktops, laptops, smartphones, tablets, gaming consoles, DVD players, TVs, etc. whose IP addresses can change often, this is a very tedious and inaccurate way to implement this feature. In addition, it is common practice for many devices to connect to the Internet through a home, business, or publicly available router. For all devices attached to such a router, the router often presents to external sites a single shared IP address using what is called Network Address Translation, or NAT. A mobile device may connect to multiple routers over the course of a single day – the home router, the coffee shop router, the work router, and back to the home router, for example. Each time a device connects to a router, it is common practice to get a new dynamically assigned IP (Dynamic Host Configuration Protocol) address internal to the router, and each router has its own unique externally presented IP address (which is what a visited web site would see).

Further complicating this approach is the transition from IPv4 to IPv6 addresses – simply speaking, there are two types of IP addresses to consider, both types are in use, and thus all sites would need to support both types. This approach is therefore extremely difficult for both users to use and for sites to implement. Essentially, all participating users would have to register all IP addresses used by all devices they connect from. In addition, they would need to update the registration every time the IP addresses change. Another affect would be that sites must check for and support both IPv4 and IPv6 type addresses, causing both users and sites to contend with network address translation (NAT). Most users do not know what their IP addresses are, how to find out what they are, how to know if they have changed, and whether or not they are subject to network address translation (which causes multiple devices to share a single IP address).

A "Do-Not-Track" Registry

A concept similar to the Do Not Track list, but basically a reverse version, would be a Do-Not-Track *Registry*. We can speculate about a "Do-Not-Track" Registry approach based on comments in a letter[5] submitted to the Federal Trade Commission in 2007 by various consumer groups when this proposal was first envisioned. That letter outlined how such a proposal would work and included the following:

> "Companies providing web, video, and other forms of browser applications should provide functionality (i.e., a browser feature, plug-in, or extension) that allows users to import or otherwise use the "do not track" list of domain names, keep the list up-to-date, and block domains on the list from tracking their internet activity."

The Do-Not-Track Registry implies advertisers would register their domains with the Federal Trade Commission. Users would install a browser plug-in and configure the plug-in by selecting what advertising domains to block. This solution requires -regulation in terms of advertisers registering the domains, and plug-in developers implementing the proper blocking mechanisms. The potential user experience disruption would be significant, and the obligation would be placed on the user to configure each device used in order to properly block tracking. Again, looking at the future of Internet browsing habits and the fluidity of how a user may transition

[5] Letter submitted to Donald S. Clark, Secretary of the U.S. Federal Trade Commission in advance of the FTC Town Hall, "Ehavioral Advertising: Tracking, Targeting, and Technology," held November 1-2, 2007 in Washington, D.C. by Ari Schwartz, Deputy Director, Center for Democracy and Technology; Linda Sherry, Director, National Priorities Consumer Action; Mark Cooper, Director of Research, Consumer Federation of America; Lee Tien, Senior Staff Attorney, Electronic Frontier Foundation; Deborah Pierce, Executive Director, Privacy Activism; Daniel Brandt, President, Public Information Research; Robert Ellis Smith, Publisher, Privacy Journal; Beth Givens, Director, Privacy Rights Clearinghouse; and Pam Dixon, Executive Director, World Privacy Forum.

from one device to another throughout the day, this solution forces the user to configure each device used to browse the Internet in what is likely an unrealistic way. Additional hurdles are in play when shared computers are used. For example, how would a Do-Not-Track Registry work in a library or hotel business center, where each user may have different tracking preferences?

The Browser Header Attribute "x-notrack"

One solution described by researchers looks at an HTTP header attribute sent by the browser to tracking servers describing the user's preference in tracking. The user would configure the browser at first launch defining the tracking preferences for the session. The setting would set the "x-notrack" attribute in the browser header. Actions by the browser alone, however, are not sufficient to protect the user. There is also a need to involve a server component in the solution. Here the advertising servers feeding advertisements would need to honor the browser header attribute for no tracking. Federal Trade Commission regulation in this case would not allow advertisers to set any persistent tracking cookies on the user system.

At first glance, this solution seems simple enough; but after working through implementation scenarios, we would likely begin to see a bifurcation of internet activity. A user with the no-track option enabled may be fed Web sites with limited content, while other users without the option set would see a richer web page and have a more robust browsing experience. A user may chose to allow first-party tracking in exchange for a more feature rich experience, for example, while preventing tracking from third party sites. By looking at configuration silos (first party tracking vs. third party tracking), we quickly move into the conflicts between End User License Agreements (EULAs) and Do-Not-Track/No-Track options.

The focus thus far has been on browser tracking habits, but are we limiting the tracking activities to only advertisers or are we addressing any and all tracking done on a device? With many day-to-day computer applications, when a user decides to use an application, the user accepts the EULA in order to complete installation. If the product tracks certain user activities, as is often the case, does the EULA now trump the Do-Not-Track option?

The real crux is this: How far would a "do-not-track" concept go? Is it limited to advertising and Web sites, or does it extend to ANY type of tracking? What about tracking in order to enforce licensing restrictions (is this software being used by the person it is licensed to, and only that person)? Is it okay to track usage patterns anonymously so that we can improve the usability of our product? Is it okay for us to identify a particular computer or user, but only anonymously so that we can implement our reputation security system as long as the tracked information cannot be tracked back to a specific user? It is not just what can be tracked "on a device", but in combination between the device and observable attributes from the server side.

Until we can see a formal proposal by the Federal Trade Commission, it is difficult to access the merits and the technical specifications of a Do-Not-Track proposal. Details are also sparse about how a Do-Not-Track mechanism might actually be implemented. What is clear, though, is that there are a variety of possible technical and regulatory approaches to the problem, each with its own difficulties and limitations -- many of which could potentially unintentionally impact cyber security.

We believe that consumers should have the right to visit or not visit a website as they see fit. Consumers already have protections, some provided directly from advertising organizations, as well as browser based

security protections, and anti-virus options to keep cookies, software, and other unwanted materials off of their systems.

Right now, implementing the same framework as used for the Do Not Call registry does not appear to be the best solution for today's online world. The comparison is still useful though, if only to caution against the assumption that Do-Not-Track will be as easy, or as successful, as Do Not Call. The differences between the problems at hand and the technologies involved are substantial. As mentioned earlier, the focus should not be in limiting technology and user experiences online but focused on the malicious behaviors that impact user safety and security while transacting online.

We are unsure exactly how a Do-Not-Track mechanism would be all that different from the opt-out link currently offered by the Network Advertising Initiative (NAI). Perhaps the most significant difference might be that the NAI includes only a limited number of companies, but a Do-Not-Track registry would presumably be universal. Given the technical challenges of a Do-Not-Track registry, we would instead recommend that Congress, the Federal Trade Commission, the Department of Commerce and private sector stakeholders participate in an effort to develop a voluntary but enforceable code of conduct. Companies that adhere to those voluntary principles could be given incentives to comply such as safe harbor protection.

Our approach to preventing and tracing cyber attacks includes improving identification and authentication of those who seek access to the system that must be protected. Our vision is for a future where individuals can voluntarily choose to obtain a secure, interoperable, and privacy-enhancing credential such as a smart identity card or a digital certificate on a cell phone, from a variety of public and private service providers, to authenticate themselves online for different types of transactions.

Symantec also supports efforts similar to those being pursued by the White House with the development of the "National Strategy for Trusted Identities in Cyberspace" (NSTIC), which seeks an online environment where individuals and organizations can complete online transactions with confidence, trusting each other's identities and the infrastructure upon which the transaction runs.

One of the challenges of a Do-Not-Track concept is that privacy, while not entirely arbitrary, is highly malleable and sensitive to non-normative factors. Understanding the value that individuals assign to the protection of their personal data is of great importance to policy makers, businesses, and researchers. What one user considers excessive tracking might be completely reasonable to others. A consumer may prefer that a trusted site tracks their online interactions, as this may result in a richer user experience and in more relevant messaging; but that same consumer may not want to be tracked by certain other sites or vendors.

Individual privacy preferences make a Do-Not-Track mechanism—or any other one size fits all approach—a rather awkward fit no matter how implemented. Users need simplicity, but it is doubtful that simple controls can adequately capture the nuances of individual privacy preferences.

Conclusion

The actions of many adware and spyware programs go beyond simply facilitating advertisements or gathering aggregate non-personally-identifiable data. Many adware and spyware programs use techniques akin to malicious threats from social engineering to exploit vulnerabilities. Once installed on the system, they use techniques to hide themselves and prevent their removal. In addition, many adware and spyware programs

gather personally-identifiable and confidential data and are able to correlate that data continually to build marketing profiles.

Overall user attitudes toward privacy, performance, ease of removal, and newly introduced spyware or adware program's characteristics will determine how they want their security product to deal with each individual situation. User expectations of computer virus protections have traditionally been for the product to assess functionality and risk, and then to make globally appropriate decisions on disinfection or removal of the viral threat. As the landscape has grown and evolved, however, a more user-centric approach is required. Thus, a useful approach is to detect all of these risks in a way that is non-intrusive, then to allow the user to make informed decisions based upon their own level of accepted risk.

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.

The government should encourage private sector stakeholders to participate in an effort to develop a voluntary but enforceable code of conduct. Companies that adhere to those voluntary principles should be given incentives to comply such as safe harbor protection.

One safe harbor that Congress should consider including is a "Good Samaritan" provision for developers of anti-spyware solutions which are providing effective protection to computer users against online threats. Unfortunately, developers often are threatened with lawsuits for defamation and interference with their business by purveyors of spyware and harmful adware. These spurious threats force anti-spyware companies to divert 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.

Right now, applying the Do Not Call framework to the Internet does not appear to be the best solution for today's online world. The problems at hand and the technologies involved are substantial. One of the challenges of a Do-Not-Track concept is that privacy, while not entirely arbitrary, is highly malleable and sensitive to non-normative factors. Individual privacy preferences are arbitrary and would make a one-size-fits-all Do-Not-Track mechanism an impossible standard to establish.

Congress should instead focus on creating privacy policies which help foster an online trusted environment where individuals and organizations can complete online transactions with confidence, trusting each other's identities and the infrastructure that the transaction runs on.

Thank you for the opportunity to testify before the Committee today on the issues of privacy, online advertising and the concept of a Do-Not-Track registry. Symantec looks forward to continuing to work with Congress as these important issues move forward.