Testimony of

Vincent Weafer

Vice President, Security Response

Symantec Corporation

On behalf of

Symantec Corporation
& the
Business Software Alliance (BSA)

On

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

Before the

U.S. Senate Committee on Commerce, Science and Transportation

Washington, D.C.

June 11, 2008

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.

[1] BSA 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.

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.

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 email 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 antispyware/antivirus 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 web-sites is less likely to be detected. Site-specific vulnerabilities are perhaps the most telling indication of this trend. During the last six 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 six 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 email 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, HR 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 US 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 USC 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 <u>not</u> seeking unlimited protection. We <u>fully</u> agree that good faith and due process <u>must</u> be applied by an anti-spyware provider when his product targets a software application for removal by the computer user.

[2] The Bill Emerson Good Samaritan Food Donation Act (42 USC 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 USC 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 USC 1) precludes liability arising from statements and disclosures regarding the Y2K problem, except in cases of recklessness or intent to deceive.

[3] Zango has appealed the ruling and BSA, as well as several other online consumer protection organizations such as the Anti-Spyware 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.

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 HR 964 last year. It would thus provide a strong foundation for the Senate to work with the House towards 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 dollars in losses to the software industry each year, including more than 8 billion dollars in the US 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 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.