Testimony of

Robert Holleyman, II

President & CEO

Business Software Alliance (BSA)

On

E-SPYING: BAN BEHAVIOR NOT TECHNOLOGY

Before the

Subcommittee on Communications

Senate Commerce, Science and Transportation Committee

Washington, D.C.

March 23, 2004

Good morning. Thank you very much for the opportunity to testify here today. My name is Robert Holleyman and I am President and CEO of the Business Software Alliance (BSA).*

BSA represents the world's leading developers of software, hardware and Internet technologies both in the U.S. and internationally. Our mission is to educate computer users on software copyrights and cyber security, advance public policy that fosters innovation and expands trade opportunities, and fight software piracy. We are headquartered in Washington, D.C., and are active in over 65 countries internationally.

It is a pleasure to be with you today to discuss a serious issue of consumer protection: protecting millions of computer users from those who secretly install software on computers in order to obtain information about those users. Such software goes by the name of "spyware." That is clearly the intent of the SPY BLOCK Act (S.2145) introduced by Chairman Burns and Senators Wyden and Boxer. It also is the intent of the Safeguard Against Privacy Invasions Act (H.R. 2929) introduced by Representatives Bono and Towns.

Mr. Chairman, you and the other members of this Committee have been leaders in adapting our laws to the information age -- carefully and deliberately, with a scalpel not a saw. This morning I would like to make three points.

*.BSA members include Adobe, Apple, Autodesk, Avid, Bentley Systems, Borland, Cisco Systems, CNC Software/Mastercam, HP, IBM, Intel, Internet Security Systems, Intuit, Macromedia, Microsoft, Network Associates, PeopleSoft, RSA Security, SolidWorks, Sybase, Symantec, UGS PLM Solutions and VERITAS Software.

First, computer snooping, or spying on computer users, is a reprehensible practice that invades our privacy. However, the problem is with bad behavior, not bad software tools or products.

Second, for that reason Congress should continue to ban the behavior not the technology. The problem is with abuse, not use, of technology.

Third, we believe the bills as introduced can be improved by focusing more directly on punishing the behavior rather than the means by which it is accomplished. Such an approach enables Congress to avoid having to make very difficult decisions about the design and operation of technology.

Stop E-Spying

We agree with the members of this Committee, other Members of Congress, and the public who rightfully complain about those who hijack computers. There is no policy rationale to justify the actions of those who secretly insert a computer program into someone's PC in order to collect information about that individual or his or her computer habits. It is, pure and simple, an invasion of our privacy. It is wrong and it should be stopped. It is also a national problem and needs a national solution.

Clearly some of these invasions of privacy are intended to, and do, cause economic harm. Someone might be trying to gain insider business information or corporate secrets. Others might be engaged in identity theft – a practice that is estimated

to cost American consumers more than $50 billion each year. But electronic snooping is no less invasive if the information is being gathered "only" for marketing or research purposes.

Ban Behavior Not Technology

It is essential that we recognize that the problem comes from bad people, not bad products. The same underlying technology that can enable spyware also may power many legitimate applications that benefit millions of computer users everyday.

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 a crime. And last year Congress did not ban telephones because some people use them to make unwanted marketing calls. Instead, Congress addressed the offensive behavior and established procedures to control telemarketing.

Mr. Chairman, I feel like I am preaching to the choir. The Commerce Committee has been a leader in applying this principle to developing computer technologies.

Just last year you moved aggressively and appropriately to "CAN-SPAM." That legislation criminalized fraudulent conduct and established clear rules for legitimate business to follow. It made it illegal to access a computer without authorization and use it to send out bulk unsolicited commercial electronic mail or to hide or falsify information

about the sender or subject matter of spam. The Act also required the inclusion of a functioning return email address and a prohibition on sending messages to recipients who opt not to receive them. It also addressed more "aggravated violations" such as the use of harvested addresses or the automated creation of multiple electronic mail accounts. But what the bill did not do is to get in the way of the continued development of innovative technological solutions to combat spam and protect consumers.

Mr. Chairman, this committee also successfully applied this principle during the encryption battles of the 1990's. You understood well that it was pointless to try and ban a technology prevalent around the world. Your "PRO-CODE" bill in 1996 prohibited the government from designing and mandating encryption standards and promoted the use of commercial encryption. At the same time, you also agreed with Senator Leahy in his legislation, as well as the House bill introduced by Representatives Goodlatte and Lofgren (the "SAFE" Bill), that it was unlawful to use encryption in the commission of a crime.

Even the Communications Decency Act of 1996 (Title V of the Telecommunications Act of 1996), which among other things sought to address the problem of on-line pornography and minors, did <u>not</u> ban the then emerging "interactive computer service." Instead the Act criminalized the use of such a service to send or display obscene and indecent content to those under 18. The Act also established a defense for those who in good faith took reasonable, effective and appropriate actions to restrict or prevent access by minors (including technological means to do so --) but

precluded the FCC from endorsing, approving, sanctioning or permitting particular products.

This built on the underlying approach of the 1984 Computer Fraud & Abuse Act which has been amended many times since to expand and strengthen its criminal and civil penalties against computer abusers. This statute penalizes those who access a computer without appropriate authorization and cause broadly defined damage. This statute addresses both those who trespass in cyberspace for commercial gain as well as those who seek to cause harm by launching computer viruses. Indeed, one possible solution to the problem of electronic snooping would be to make illicit the act of commercializing information obtained through surreptitious means.

Why has Congress consistently prohibited conduct not technology? Why has Congress refrained from interfering with the marketplace by dictating the design or operations of computers and consumer electronics?

Congress has wisely avoided technology mandates because you understand that the U.S. technology industry is 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 and hurts users of technology products by stifling innovation, freezing in place particular technologies, impairing product performance, and increasing consumer costs.

Focus and Improve The Legislation

We believe the pending legislation should be changed to focus even more clearly on what we are trying to stop, not the technology tools to do so. We also think that the most immediate, concrete and compelling problem is electronic spying – the unauthorized acquisition and use of information from individuals.

Currently the SPY BLOCK bill has numerous definitions, requirements and exemptions which involve making technical decisions about the operations of today's computers – as well as the direction of future technology. The bill:

- attempts to define computer software, cookie, install; network information; information collection feature, advertising feature, distributed computing feature, and settings modification feature;
- in the case of advertising, distributed computing, and settings modification features requires descriptions of how those features will operate on, and with, a particular computer (e.g. "the nature, volume of information or messages, and the likely impact on the computer's processing capacity of any computational or processing tasks the computer software will cause the computer to perform…") ;
- directs certain technical uninstall operations; and
- necessarily seeks to exempt "any feature of computer software that is reasonably needed to provide capability for general purpose online browsing, electronic mail, or instant messaging…determine whether or not the user of computer is licensed or authorized to use the computer software and provide

technical support for the use of the computer software by the user of the computer."

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 unauthorized acquisition and commercialization of information.

We suggest that Congress simply prohibit the distribution in interstate commerce of user information obtained electronically from an individual's computer, unless the person seeking to sell the information can show that it was collected with user's explicit permission or that it was obtained from an unaffiliated entity that represents it had collected the information with such permission. Such an approach significantly mitigates the definitional issues in the bill as introduced -- and their implications for the development and use of technology -- while achieving the objectives of the legislation.

We also believe that what the bill calls advertising, distributed computing, and settings modification features should not be included in this legislation. None of these issues has risen to the same level of concern or been examined nearly as much as electronic spying. Each of these areas also raises separate and distinct substantive and political issues.

For example, having just spent nearly a year implementing legislation to control spam, we are concerned that additional legislation on advertising at this point would detract from the current focus on spying. We also think it is worthwhile to more closely

examine existing laws that address deceptive advertising and business practices. Similarly, the case of distributed computing raises new questions. We understand the concern about "zombie" machines utilized without consent – as opposed to the enthusiastic voluntary participation of tens of thousands in the search for extraterrestrial intelligence (the SETI project). But the concept of "grid computing" is just emerging as a serious commercial enterprise and we would be hesitant to casually address it in this bill. Finally, we believe the area of settings as well as their modification is integrally related to on-going efforts to address cybersecurity concerns. Once again, we would be reluctant to address those issues in this bill. As many of the Committee's members know, BSA has been extremely active in efforts to making computing safer and more secure. BSA was one of the hosts and cosponsors of the Department of Homeland Security Cybersecurity Summit last December and throughout this month we are announcing the significant results from private sector efforts initiated at the summit.

More generally, we note that each of these areas may also be amenable to technological and business practices. We think Congress should be careful not to preclude the evolution of tools and marketplace solutions.

With respect to enforcement, we agree that the FTC should be given primary responsibility. The FTC should treat violations as an unfair or deceptive act under the FTC Act. We understand that other regulatory agencies may have enforcement responsibility in other areas.

We also believe that the Department of Justice should be authorized and empowered to subject those who violate the legislation to criminal fees and imprisonment under Title 18 of the United States Code. We should send a clear message that engaging in electronic spying is reprehensible and will not be tolerated.

However, we think that the State Attorneys General should be given enforcement authority in this area only if we have a federal standard. Remote access electronic spying through "spyware" is a national problem. We think it should be treated as such. The obvious problems with empowering State Attorneys General in the absence of a federal standard is the prospect for many different enforcement actions based on many different theories and many different standards.

Conclusion

Thank you again for this opportunity to comment on the issue of "spyware" and the SPY BLOCK bill. Working together, I believe the bill can be improved to more directly and effectively address the issue we are all most concerned about: electronic spying.